

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor: : Masaaki TAKASE  
Filed : Concurrently herewith  
For : KEY EXCHANGE PROXY....  
Serial No. : Concurrently herewith

September 30, 2003


Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

PRIORITY CLAIM AND  
SUBMISSION OF PRIORITY DOCUMENT

S I R:

Applicant hereby claims priority under 35 USC 119 from **Japanese** patent application number **2002-288476** filed **October 1, 2002**, a copy of which is enclosed.

Respectfully submitted,

  
\_\_\_\_\_  
Thomas J. Bean  
Reg. No. 44,528

Katten Muchin Zavis Rosenman  
575 Madison Avenue  
New York, NY 10022-2585  
(212) 940-8800  
Docket No.: FUJH 20.637

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日  
Date of Application: 2 0 0 2 年 1 0 月 1 日

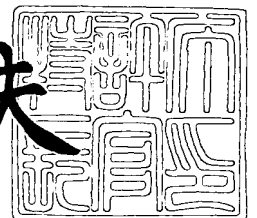
出 願 番 号  
Application Number: 特 願 2 0 0 2 - 2 8 8 4 7 6  
[ST. 10/C]: [ J P 2 0 0 2 - 2 8 8 4 7 6 ]

出 願 人  
Applicant(s): 富士通株式会社

2 0 0 3 年 8 月 1 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫



出証番号 出証特 2 0 0 3 - 3 0 6 1 9 0 5

【書類名】 特許願

【整理番号】 0251633

【提出日】 平成14年10月 1日

【あて先】 特許庁長官 殿

【国際特許分類】 H04L 9/08  
G09C 1/00

【発明の名称】 鍵交換代理ネットワークシステム

【請求項の数】 10

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 高瀬 正明

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100094514

【弁理士】

【氏名又は名称】 林 恒徳

【選任した代理人】

【識別番号】 100094525

【弁理士】

【氏名又は名称】 土井 健二

【手数料の表示】

【予納台帳番号】 030708

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9704944

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 鍵交換代理ネットワークシステム

【特許請求の範囲】

【請求項 1】 暗号通信を行う第 1 および第 2 の端末装置の間で行われる鍵交換処理を代行する鍵交換代理ネットワークシステムであって、

前記第 1 の端末装置にアクセスされる第 1 のサービス制御装置および前記第 1 の端末装置の鍵交換処理を代行する第 1 の鍵交換代理装置を備え、

前記第 1 のサービス制御装置は、

前記第 1 もしくは第 2 の端末装置または前記第 1 の鍵交換代理装置からのメッセージを受信する第 1 のメッセージ受信部と、

前記第 1 のメッセージ受信部により受信されたメッセージが鍵交換メッセージまたは鍵を含むメッセージかどうかを判断するための第 1 のデータを保持し、該第 1 のデータに基づいて前記受信メッセージが前記鍵交換メッセージまたは前記鍵を含むメッセージかどうかを判断し、前記受信メッセージが前記第 1 または第 2 の端末装置からの鍵交換メッセージの場合には転送先を前記第 1 の鍵交換代理装置とし、前記受信メッセージが前記第 1 の鍵交換代理装置からの鍵交換メッセージの場合には転送先を前記第 2 の端末装置とし、前記受信メッセージが前記鍵を含むメッセージの場合には転送先を前記第 1 の端末装置として決定する第 1 のプロトコル制御部と、

前記第 1 のプロトコル制御部により決定された転送先に前記第 1 のメッセージ受信部により受信されたメッセージを送信する第 1 のメッセージ送信部と、

を備え、

前記第 1 の鍵交換代理装置は、

前記第 1 のサービス制御装置からのメッセージを受信する第 2 のメッセージ受信部と、

前記第 2 のメッセージ受信部により受信されたメッセージが前記鍵交換メッセージである場合に、前記第 2 の端末装置との間で前記鍵交換メッセージを交換して鍵を決定する第 2 のプロトコル制御部と、

前記第 2 のプロトコル制御部により決定された前記鍵を、前記鍵を含むメッセ

ージとして前記第 1 のサービス制御装置宛てに送信する第 2 のメッセージ送信部と、

を備えている鍵交換代理ネットワークシステム。

【請求項 2】 請求項 1 において、

前記第 2 のプロトコル制御部は、前記第 1 の端末装置からの鍵交換メッセージの受信を契機として前記第 2 の端末装置との間で鍵を決定する、鍵交換ネットワークシステム。

【請求項 3】 請求項 1 において、

前記第 2 のプロトコル制御部は、前記第 2 の端末装置からの鍵交換メッセージの受信を契機として前記第 2 の端末装置との間で鍵を決定する、鍵交換ネットワークシステム。

【請求項 4】 請求項 1 から 3 のいずれか 1 項において、

前記第 2 の端末装置にアクセスされる第 2 のサービス制御装置および前記第 2 の端末装置の鍵交換処理を代行する第 2 の鍵交換代理装置をさらに備え、

前記第 2 のサービス制御装置は、

前記第 1 もしくは第 2 の端末装置または前記第 2 の鍵交換代理装置からのメッセージを受信する第 3 のメッセージ受信部と、

前記第 3 のメッセージ受信部により受信されたメッセージが鍵交換メッセージまたは鍵を含むメッセージかどうかを判断するための第 2 のデータを保持し、該第 2 のデータに基づいて前記受信メッセージが前記鍵交換メッセージまたは前記鍵を含むメッセージかどうかを判断し、前記受信メッセージが前記第 1 または第 2 の端末装置からの鍵交換メッセージの場合には転送先を前記第 2 の鍵交換代理装置とし、前記受信メッセージが前記第 2 の鍵交換代理装置からの鍵交換メッセージの場合には転送先を前記第 1 の端末装置とし、前記受信メッセージが前記鍵を含むメッセージの場合には転送先を前記第 2 の端末装置として決定する第 3 のプロトコル制御部と、

前記第 3 のプロトコル制御部により決定された転送先に前記第 3 のメッセージ受信部により受信されたメッセージを送信する第 3 のメッセージ送信部と、

を備え、

前記第 2 の鍵交換代理装置は、

前記第 2 のサービス制御装置からのメッセージを受信する第 4 のメッセージ受信部と、

前記第 4 のメッセージ受信部により受信されたメッセージが前記鍵交換メッセージである場合に、前記第 1 の鍵交換代理装置との間で前記鍵交換メッセージを交換して鍵を決定する第 4 のプロトコル制御部と、

前記第 4 のプロトコル制御部により決定された前記鍵を、前記鍵を含むメッセージとして前記第 2 のサービス制御装置宛てに送信する第 4 のメッセージ送信部と、

を備えている鍵交換代理ネットワークシステム。

【請求項 5】 請求項 4 において、

前記第 1 および第 2 のサービス制御装置が同一の装置により構成される、鍵交換代理ネットワークシステム。

【請求項 6】 暗号通信を行う第 1 および第 2 の端末装置の間で行われる鍵交換処理を代行する鍵交換代理ネットワークシステムであって、

前記第 1 の端末装置にアクセスされるサービス制御装置および前記第 1 の端末装置の鍵交換処理を代行する鍵交換代理装置を備え、

前記サービス制御装置は、受信メッセージの転送先を判断するためのサービスプロファイルに基づいて、前記第 1 の端末装置からの鍵交換代理要求メッセージまたは前記第 2 の端末装置からの鍵交換メッセージを前記鍵交換代理装置に転送し、前記鍵交換代理装置からの鍵交換メッセージを前記第 2 の端末装置に転送するとともに、前記鍵交換代理装置からの鍵を含むメッセージを前記第 1 の端末装置に転送し、

前記鍵交換代理装置は、前記鍵交換メッセージを前記第 2 の端末装置との間で前記サービス制御装置を介して交換して鍵を決定し、決定した鍵を含むメッセージを前記サービス制御装置を介して前記第 1 の端末装置に送信する、

鍵交換代理ネットワークシステム。

【請求項 7】 端末装置によりアクセスされ、該端末装置、該端末装置の鍵交換処理を代行する鍵交換代理装置、または該端末装置と暗号通信を行う通信相

手端末からのメッセージを転送するサービス制御装置であって、

前記端末装置、前記鍵交換代理装置、または前記通信相手端末装置からのメッセージを受信するメッセージ受信部と、

前記メッセージ受信部により受信されたメッセージが鍵交換メッセージまたは鍵を含むメッセージかどうかを判断するためのデータを保持し、該データに基づいて前記受信メッセージが前記鍵交換メッセージまたは前記鍵を含むメッセージかどうかを判断し、前記受信メッセージが前記端末装置または通信相手端末装置からの鍵交換メッセージの場合には転送先を前記鍵交換代理装置とし、前記受信メッセージが前記鍵交換代理装置からの鍵交換メッセージの場合には転送先を前記通信相手端末装置とし、前記受信メッセージが前記鍵を含むメッセージの場合には転送先を前記端末装置として決定するプロトコル制御部と、

前記プロトコル制御部により決定された転送先に前記受信メッセージを送信するメッセージ送信部と、

を備えているサービス制御装置。

【請求項 8】 通信相手端末装置と暗号通信を行う端末装置に代わって前記通信相手端末との間で鍵交換処理を行う鍵交換代理装置であって、

前記端末装置にアクセスされ、前記端末装置または前記通信相手端末装置からのメッセージを転送するサービス制御装置からのメッセージを受信するメッセージ受信部と、

前記メッセージ受信部により受信されたメッセージが鍵交換メッセージである場合に、前記通信相手端末装置との間で前記鍵交換メッセージを交換して鍵を決定するプロトコル制御部と、

前記プロトコル制御部により決定された前記鍵を、前記鍵を含むメッセージとして前記サービス制御装置宛てに送信するメッセージ送信部と、

を備えている鍵交換代理装置。

【請求項 9】 通信ネットワークのサービス制御装置にアクセスして、通信相手端末装置と暗号通信を行う端末装置であって、

暗号化が必要な通信の条件を規定した第 1 のデータおよび暗号化に使用される鍵を含む第 2 のデータを保持し、前記第 1 のデータに基づいて通信相手端末装置



との通信に暗号化が必要かどうかを判断し、暗号化に必要な鍵が前記第2のデータに存在するかどうかを判断する暗号処理管理部と、

前記暗号処理管理部により暗号化が必要であると判断され、かつ、暗号化に必要な鍵が存在しないと判断された場合に、鍵交換メッセージを前記サービス制御装置を介して前記通信相手端末宛てに送信するメッセージ送信部と、

前記通信ネットワークの鍵交換代理装置と前記通信相手端末装置との間で決定された鍵を含むメッセージを前記サービス制御装置から受信するメッセージ受信部と、

を備えている端末装置。

【請求項10】 暗号通信を行う第1および第2の端末装置の間で行われる鍵交換処理を前記第1の端末装置に代わって行う鍵交換代理装置および前記第1の端末装置にアクセスされるサービス制御装置を有する鍵交換代理ネットワークシステムで実行される鍵交換代理方法であって、

前記サービス制御装置において、前記第1または第2の端末装置から送信される鍵交換メッセージを前記鍵交換代理装置に転送し、

前記鍵交換代理装置において、前記第1の端末装置と前記第2の端末装置との間で交換される鍵交換メッセージを作成して前記サービス制御装置に送信し、

前記サービス制御装置において、前記鍵交換メッセージを前記第2の端末装置に転送し、

前記鍵交換代理装置において、前記鍵交換メッセージの交換により決定された鍵を含むメッセージを前記サービス制御装置に送信し、

前記サービス制御装置において、前記鍵交換代理装置から送信された前記鍵を含むメッセージを前記第1の端末装置に転送する、

鍵交換代理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、通信端末間での暗号鍵の交換を代理する鍵交換代理ネットワークシステムに関し、特に、IPSecにおいて必要となる鍵の交換を代理する鍵交換

代理ネットワークシステムに関する。

#### 【0002】

また、本発明は、鍵交換代理ネットワークシステムにおける端末装置、サービス制御装置、および鍵交換代理装置に関する。

#### 【0003】

##### 【従来の技術】

インターネットの急速な発展により IP パケットのトラフィックが急増している。また、携帯電話の普及に伴い、IMT-2000 (International Mobile Telecommunications 2000) での標準化、実用化の動きもあり、モバイル環境での高速 IP 通信が普及すると考えられる。

#### 【0004】

モバイル環境での IP 通信では、従来の IPv4 ではアドレス枯渇の問題があるので、IPv6 が必須となっている。この IPv6 環境では、サーバ等の端末に IPSec / IKE (IP Security / Internet Key Exchange) が必須となっているので、IPSec を用いた安全な通信が提供され则认为られる。

#### 【0005】

しかし、IPSec / IKE では、端末に鍵交換サーバ (IKE サーバ) を搭載する必要がある。この鍵交換サーバは複雑な処理を行うため、端末には、比較的高速な処理装置 (CPU 等) と大きなメモリが必要となる。

#### 【0006】

したがって、パソコンやサーバ等の端末には、IPSec / IKE の導入が容易である一方、小型軽量化が要求される携帯電話や PDA (Personal Digital Assistant) 等の携帯端末に IPSec / IKE を導入するには、難点がある。

#### 【0007】

たとえば、一般的に安全でない通信路で安全に鍵交換を行う方法として Diffie-Hellman の鍵交換方法があるが、この方法を実行するには、鍵交換を行う端末においてべき乗計算を行う必要があるため、端末のリソースを消費し、携帯端末には大きな負荷となる。

#### 【0008】

また、IPSec/IKEの処理には電力を多く必要とするので、携帯端末における消費電力という観点からも、IPSec/IKEを携帯端末に搭載するのは現実的ではない。このため、携帯端末自身にはなるべく機能追加を行わずに、IPSec/IKEによるサービスを行うことが求められている。

#### 【0009】

そこで、鍵交換処理を携帯端末が行うのではなく、他の装置に代行させる技術が考えられ、このような技術として、ユーザ端末機器からアクセスされるホームサーバ等の装置が代行するものがある（たとえば、特許文献1参照）。

#### 【0010】

##### 【特許文献1】

特開2002-158650号公報（図1等）

#### 【0011】

##### 【発明が解決しようとする課題】

しかし、この従来の技術によると、ユーザ端末機器がホームサーバ等の代行サーバに直接アクセスするので、ユーザ端末機器は代行サーバのアドレスを知っている必要がある。この場合に、ユーザ端末機器と通信を行う相手端末機器は、必ずしも代行サーバのアドレスを知っているとは限らないので、相手端末機器から通信を開始して鍵交換を行うことはできない。したがって、適用の範囲が、ユーザ端末機器から通信を開始する場合に限定される。

#### 【0012】

本発明は、このような背景に鑑みなされたものであり、その目的は、鍵交換に伴う処理をネットワーク側の装置に代行させて、端末の負荷を軽減することにある。

#### 【0013】

また、本発明の目的は、暗号通信を行う2つの端末のいずれから鍵交換処理の要求があっても鍵交換処理の代行が可能な鍵交換方式を提供することにある。

#### 【0014】

##### 【課題を解決するための手段】

前記目的を達成するために、本発明による鍵交換代理ネットワークシステムは

、暗号通信を行う第1および第2の端末装置の間で行われる鍵交換処理を代行する鍵交換代理ネットワークシステムであって、前記第1の端末装置にアクセスされる第1のサービス制御装置および前記第1の端末装置の鍵交換処理を代行する第1の鍵交換代理装置を備え、前記第1のサービス制御装置は、前記第1もしくは第2の端末装置または前記第1の鍵交換代理装置からのメッセージを受信する第1のメッセージ受信部と、前記第1のメッセージ受信部により受信されたメッセージが鍵交換メッセージまたは鍵を含むメッセージかどうかを判断するための第1のデータを保持し、該第1のデータに基づいて前記受信メッセージが前記鍵交換メッセージまたは前記鍵を含むメッセージかどうかを判断し、前記受信メッセージが前記第1または第2の端末装置からの鍵交換メッセージの場合には転送先を前記第1の鍵交換代理装置とし、前記受信メッセージが前記第1の鍵交換代理装置からの鍵交換メッセージの場合には転送先を前記第2の端末装置とし、前記受信メッセージが前記鍵を含むメッセージの場合には転送先を前記第1の端末装置として決定する第1の Protokol 制御部と、前記第1の Protokol 制御部により決定された転送先に前記第1のメッセージ受信部により受信されたメッセージを送信する第1のメッセージ送信部と、を備え、前記第1の鍵交換代理装置は、前記第1のサービス制御装置からのメッセージを受信する第2のメッセージ受信部と、前記第2のメッセージ受信部により受信されたメッセージが前記鍵交換メッセージである場合に、前記第2の端末装置との間で前記鍵交換メッセージを交換して鍵を決定する第2の Protokol 制御部と、前記第2の Protokol 制御部により決定された前記鍵を、前記鍵を含むメッセージとして前記第1のサービス制御装置宛てに送信する第2のメッセージ送信部と、を備えている。

#### 【0015】

本発明による鍵交換代理ネットワークシステムは、通信相手端末装置と暗号通信を行う端末装置に代わって前記通信相手端末との間で鍵交換処理を行う鍵交換代理装置であって、前記端末装置にアクセスされ、前記端末装置または前記通信相手端末装置からのメッセージを転送するサービス制御装置からのメッセージを受信するメッセージ受信部と、前記メッセージ受信部により受信されたメッセージが鍵交換メッセージである場合に、前記通信相手端末装置との間で前記鍵交換

メッセージを交換して鍵を決定するプロトコル制御部と、前記プロトコル制御部により決定された前記鍵を、前記鍵を含むメッセージとして前記サービス制御装置宛てに送信するメッセージ送信部と、を備えている。

#### 【0016】

本発明による鍵交換代理方法は、暗号通信を行う第1および第2の端末装置の間で行われる鍵交換処理を前記第1の端末装置に代わって行う鍵交換代理装置および前記第1の端末装置にアクセスされるサービス制御装置を有する鍵交換代理ネットワークシステムで実行される鍵交換代理方法であって、前記サービス制御装置において、前記第1または第2の端末装置から送信される鍵交換メッセージを前記鍵交換代理装置に転送し、前記鍵交換代理装置において、前記第1の端末装置と前記第2の端末装置との間で交換される鍵交換メッセージを作成して前記サービス制御装置に送信し、前記サービス制御装置において、前記鍵交換メッセージを前記第2の端末装置に転送し、前記鍵交換代理装置において、前記鍵交換メッセージの交換により決定された鍵を含むメッセージを前記サービス制御装置に送信し、前記サービス制御装置において、前記鍵交換代理装置から送信された前記鍵を含むメッセージを前記第1の端末装置に転送する、ものである。

#### 【0017】

本発明によると、第1または第2の端末装置からサービス制御装置に送信された鍵交換メッセージは、サービス制御装置によって鍵交換代理装置に転送される。その後、鍵交換代理装置と第2の端末装置との間で鍵交換処理が行われ、暗号通信に必要な鍵が決定される。決定された鍵は第1の端末装置に送信される。

#### 【0018】

したがって、本発明によると、第1の端末装置は、鍵交換および鍵決定に必要な処理を行うことなく、暗号通信に必要な鍵を得ることができる。その結果、第1の端末装置の負荷を軽減することができる。

#### 【0019】

また、サービス制御装置は、第1または第2の端末装置からの鍵交換メッセージを鍵交換代理装置に転送する。したがって、第1の端末装置は、第2の端末装置の宛先アドレスを知っているだけでよく、また、第2の端末装置は第1の端末

装置の宛先アドレスを知っているだけでよい。このため、第1および第2の端末装置のいずれから鍵交換処理の要求があっても鍵交換処理の代行が可能である。

#### 【0020】

本発明によるサービス制御装置は、端末装置によりアクセスされ、該端末装置、該端末装置の鍵交換処理を代行する鍵交換代理装置、または該端末装置と暗号通信を行う通信相手端末からのメッセージを転送するサービス制御装置であって、前記端末装置、前記鍵交換代理装置、または前記通信相手端末装置からのメッセージを受信するメッセージ受信部と、前記メッセージ受信部により受信されたメッセージが鍵交換メッセージまたは鍵を含むメッセージかどうかを判断するためのデータを保持し、該データに基づいて前記受信メッセージが前記鍵交換メッセージまたは前記鍵を含むメッセージかどうかを判断し、前記受信メッセージが前記端末装置または通信相手端末装置からの鍵交換メッセージの場合には転送先を前記鍵交換代理装置とし、前記受信メッセージが前記鍵交換代理装置からの鍵交換メッセージの場合には転送先を前記通信相手端末装置とし、前記受信メッセージが前記鍵を含むメッセージの場合には転送先を前記端末装置として決定するプロトコル制御部と、前記プロトコル制御部により決定された転送先に前記受信メッセージを送信するメッセージ送信部と、を備えている。

#### 【0021】

本発明による鍵交換代理装置は、通信相手端末装置と暗号通信を行う端末装置に代わって前記通信相手端末との間で鍵交換処理を行う鍵交換代理装置であって、前記端末装置にアクセスされ、前記端末装置または前記通信相手端末装置からのメッセージを転送するサービス制御装置からのメッセージを受信するメッセージ受信部と、前記メッセージ受信部により受信されたメッセージが鍵交換メッセージである場合に、前記通信相手端末装置との間で前記鍵交換メッセージを交換して鍵を決定するプロトコル制御部と、前記プロトコル制御部により決定された前記鍵を、前記鍵を含むメッセージとして前記サービス制御装置宛てに送信するメッセージ送信部と、を備えている。

#### 【0022】

本発明による端末装置は、通信ネットワークのサービス制御装置にアクセスし

て、通信相手端末装置と暗号通信を行う端末装置であって、暗号化が必要な通信の条件を規定した第 1 のデータおよび暗号化に使用される鍵を含む第 2 のデータを保持し、前記第 1 のデータに基づいて通信相手端末装置との通信に暗号化が必要かどうかを判断し、暗号化に必要な鍵が前記第 2 のデータに存在するかどうかを判断する暗号処理管理部と、前記暗号処理管理部により暗号化が必要であると判断され、かつ、暗号化に必要な鍵が存在しないと判断された場合に、鍵交換メッセージを前記サービス制御装置を介して前記通信相手端末宛てに送信するメッセージ送信部と、前記通信ネットワークの鍵交換代理装置と前記通信相手端末装置との間で決定された鍵を含むメッセージを前記サービス制御装置から受信するメッセージ受信部と、を備えている。

### 【 0 0 2 3 】

#### 【発明の実施の形態】

図 1 は、本発明の実施の形態による鍵交換代理ネットワークシステムの構成を示すブロック図である。この鍵交換代理ネットワークシステムは、サービス制御装置 1、鍵交換代理サーバ 2、認証サーバ 3、ルータ 4、加入者端末 5、および通信相手端末 6 を有する。

### 【 0 0 2 4 】

サービス制御装置 1、鍵交換代理サーバ 2、認証サーバ 3、およびルータ 4 は、コアネットワーク（たとえばインターネット）7 に接続され、相互に通信可能になっている。

### 【 0 0 2 5 】

サービス制御装置 1 は、たとえばコアネットワーク 7 のエッジルータ（エッジノード）であり、モバイル IP やモバイル IP v 6 では、携帯端末（たとえば加入者端末 5）と無線通信を行うノードである。

### 【 0 0 2 6 】

サービス制御装置 1 は、鍵交換代理サーバ 2 の IP アドレスをあらかじめ知っているとともに、加入者端末 5 が位置登録を行った際に認証サーバ 3 から与えられるサービスプロファイル（後述）を保持する。

### 【 0 0 2 7 】

このサービスプロファイルにより、サービス制御装置 1 は、鍵交換処理に伴い転送すべきパケットと通常のルーティングを行うパケットとを区別し、鍵交換処理に伴い転送すべきパケット（後述する鍵交換メッセージ、鍵を含むメッセージ等）を鍵交換代理サーバ 2 または加入者端末 5 に転送する。

#### 【 0 0 2 8 】

加入者端末 5 は、たとえば携帯端末（携帯電話、PDA 等）であり、無線回線を介してサービス制御装置 1 に接続される。したがって、加入者端末 5 から送信されるパケットおよび加入者端末 5 宛てに送信されるパケットはサービス制御装置 1 を経由するようになっている。また、加入者端末 5 は、本実施の形態では、装置の小型・軽量化や低消費電力化のため、鍵交換サーバ（IKE サーバ、鍵交換プログラム）を搭載していない。

#### 【 0 0 2 9 】

通信相手端末 6 は、ルータ 4 に接続され、本実施の形態では、コアネットワーク 7 を介して加入者端末 5 と通信を行う端末である。この通信相手端末 6 は、たとえばコンピュータ、サーバ（たとえば電子商取引サーバ）等であり、鍵交換サーバ（IKE サーバ、鍵交換プログラム）を搭載している。

#### 【 0 0 3 0 】

鍵交換代理サーバ 2 は、加入者端末 5 が鍵交換サーバを搭載していないことから、加入者端末 5 に代わり、IPSec / IKE（IP Security / Internet Key Exchange）に基づいて通信相手端末 6 との間で鍵交換処理を実行し、この処理により決定された暗号鍵（共通鍵、秘密鍵等）を加入者端末 5 に与える。

#### 【 0 0 3 1 】

認証サーバ 3 は、本実施の形態では、サービス管理サーバを兼ねており、加入者端末 5 等の認証データに加えて、後に詳述するサービスプロファイル（原本）を保持する。そして、認証サーバ 3 は、加入者端末 5 のネットワーク接続の際の認証を契機としてサービスプロファイル（コピー）をサービス制御装置 1 に送信する。

#### 【 0 0 3 2 】

なお、サービスプロファイルは、認証サーバ 3 に連携した図示しないデータベ



ースに格納されてもよい。また、認証サーバ 3 とサービス管理サーバとは、個別に設けられてもよい。両サーバが個別に設けられる場合には、サービスプロファイルは、サービス管理サーバからサービス制御装置 1 に転送されることとなる。

#### 【 0 0 3 3 】

図 1 では、理解を容易にするために 1 つのサービス制御装置 1 を示しているが、コアネットワーク 7 には複数のサービス制御装置が存在し、加入者端末 5 は、その移動に伴って、一般に、最寄りのサービス制御装置と無線接続を確立する。鍵交換代理サーバもコアネットワーク 7 に複数存在してもよい。サービス制御装置および鍵交換代理サーバが複数存在する場合には、各サービス制御装置は、自己の最寄りの鍵交換代理サーバの IP アドレスを知り、最寄りの鍵交換代理サーバに加入者端末 5 の鍵交換処理を代理させることとなる。

#### 【 0 0 3 4 】

図 2 は、サービス制御装置 1 の構成を示すブロック図である。サービス制御装置 1 は、メッセージ送受信部 1 1、プロトコル制御部 1 2、およびサービス管理部 1 3 を有する。

#### 【 0 0 3 5 】

メッセージ送受信部 1 1 は、コアネットワーク 7 に接続され、コアネットワーク 7 を介して加入者端末 5、鍵交換代理サーバ 2、認証サーバ 3、ルータ 4 等からのパケット（以下「メッセージ」ともいう。）を受信し、これらの端末、サーバ、ルータ等にメッセージを送信する。

#### 【 0 0 3 6 】

プロトコル制御部 1 2 は、メッセージ送受信部 1 1 が受信したメッセージを受け取り、メッセージを解析する。そして、プロトコル制御部 1 2 は、メッセージの解析によりメッセージを転送するかどうか、および、転送する場合の転送先を決定するとともに、必要に応じてメッセージのカプセル化等を行う。

#### 【 0 0 3 7 】

このメッセージを転送するかどうかを判断するために、プロトコル制御部 1 2 は、認証サーバ 3 から与えられたサービスプロファイルを保持する。図 3 は、サービスプロファイルの一例を示している。

**【0038】**

サービスプロファイルは、ネットワーク運用者と加入者との契約に基づいて作成されるファイルであり、加入者端末（加入者）ごとに設けられる。各加入者のサービスプロファイルは、加入者識別情報および1または2以上のIPSec適用条件を有する。

**【0039】**

加入者識別情報は、加入者（加入者端末）を識別するための情報であり、たとえば電話番号、NAI（Network Access ID）、認証データベースのエントリ番号等のデータ項目を有する。

**【0040】**

IPSec適用条件は、（1）通信相手端末6から加入者端末5宛てに送信されるメッセージのうち、鍵交換代理サーバ2に転送するメッセージの条件、（2）加入者端末5から通信相手端末6宛てに送信されたメッセージのうち、鍵交換代理サーバ2に転送するメッセージの条件、または、（3）サービス制御装置1宛てに送信されたメッセージのうち、加入者端末5もしくは通信相手端末6に転送するメッセージの条件を規定したデータである。

**【0041】**

このIPSec適用条件は、IPアドレスおよびポート番号を有する。「IPアドレス」は、上記（1）～（3）の転送すべきメッセージが有する宛先IPアドレスまたは送信元IPアドレスを示す。「ポート番号」は、TCPやUDPにおけるアプリケーションを指定する番号であり、たとえば後述する鍵交換メッセージ（IKEメッセージ）には、ポート番号として500番が使用される。

サービス制御装置1は、受信したメッセージの宛先IPアドレスまたは送信元IPアドレスとIPSec適用条件のIPアドレスとが一致するかどうか、および、受信したメッセージのポート番号がIPSec適用条件のポート番号とが一致するかどうかを判断し、一致する場合にはそのメッセージの内容に応じて、そのメッセージを鍵交換代理サーバ2、加入者端末5、または通信相手端末6に転送する。

**【0042】**

転送されるメッセージは、本実施の形態では、後述するように、（１）加入者端末５から通信相手端末６宛てに送信される鍵交換メッセージ（鍵交換代理要求メッセージ）（転送先：鍵交換代理サーバ２），（２）通信相手端末６から加入者端末５宛てに送信される鍵交換メッセージ（転送先：鍵交換代理サーバ２），（３）鍵交換代理サーバ２からサービス制御装置１宛てに送信された鍵交換メッセージ（転送先：通信相手端末６），（４）鍵交換代理サーバ２からサービス制御装置１宛てに送信された鍵情報（ＳＡデータ）を含むメッセージ（転送先：加入者端末５）である。

#### 【0043】

なお、ＩＰＳｅｃ適用条件の「ＩＰアドレス」は、たとえば加入者端末５と通信する通信相手端末（通信相手端末６等）の双方のＩＰアドレスの組を示す場合もある。

#### 【0044】

サービスプロファイルは、加入者端末５が位置登録をし、認証サーバ３によって認証された時に、認証サーバ（すなわちサービス管理サーバ）３からサービス制御装置１に送信され、保持される。したがって、加入者端末５が移動し、アクセスするサービス制御装置１が変化すると、アクセスされるサービス制御装置１に認証サーバ３からサービスプロファイルが送信されることとなる。

#### 【0045】

図２に戻って、サービス管理部１３は、プロトコル管理部１２のメッセージの解析結果を受け取り、メッセージに対して行った処理等のサービスの管理する。

#### 【0046】

図４は、加入者端末５の構成を示すブロック図である。加入者端末５は、アプリケーション処理部５１，メッセージ送受信部５２，暗号化／復号化部５３，プロトコル制御部５４，および暗号処理管理部５５を有する。

#### 【0047】

アプリケーション処理部５１は、たとえばブラウザ，メール等のアプリケーションプログラムを実行し、ユーザとのインタフェース処理を実行する。そして、アプリケーション処理部５１は、ユーザの入力に基づいて、メッセージ送受信部

52にメッセージ送信要求を与えるとともに、メッセージ送受信部52により受信されたメッセージに含まれるデータを表示装置等に出力、表示等する。

#### 【0048】

メッセージ送受信部52は、コアネットワーク7に接続され、コアネットワーク7を介してサービス制御装置1からのメッセージを受信し、サービス制御装置1にメッセージを送信する。

#### 【0049】

暗号化／復号化部53は、送信メッセージの暗号化および受信メッセージの復号化を行う。プロトコル制御部54は、通信相手端末6との通信に必要な鍵が存在しない場合には、鍵交換メッセージ（鍵交換代理要求メッセージ）を生成し、また、セキュリティアソシエーション（SA：Security Association）データを含むメッセージ（鍵メッセージ）を鍵交換代理サーバ2から受信した場合には、受信メッセージからSAデータを抽出する。

#### 【0050】

暗号処理管理部55は、セキュリティポリシーデータベース（SPD：Security Policy Database）およびセキュリティアソシエーションデータベース（SAD：Security Association Database）を保持し、これらのデータに基づいて通信相手端末6との通信に暗号化が必要かどうかや鍵の有無を判断する。

#### 【0051】

図5（A）は、加入者端末5の暗号処理管理部55に保持されるSPDを示し、同図（B）は加入者端末5の暗号処理管理部55に保持されるSADを示している。

#### 【0052】

SPDは、加入者端末5にIPSecによる暗号化通信を適用するための1または2以上のIPSec適用条件を含んでいる。各IPSec適用条件は、その内容として、前述したサービスプロファイル（図3参照）と同様に、IPアドレスおよびポート番号を有する。「IPアドレス」は、暗号化通信が必要とされる通信相手端末のIPアドレスであり、「ポート番号」は、暗号化通信が必要とされるポート番号（TCPやUDPにおけるアプリケーションを指定する番号）であ

る。

#### 【0053】

加入者端末5がこれらIPアドレスおよびポート番号と一致するパケットを送信する場合に、その送信パケットにはIPSec/IKEによる暗号化通信が適用される。

#### 【0054】

SADは、1または2以上のセキュリティアソシエーションデータ(SAデータ)からなる。各SAデータは、適用条件および内容を有する。「適用条件」は、SPDの適用条件と同様のIPアドレスおよびポート番号を有する。「内容」は、暗号化通信に使用される暗号化方法(暗号化プロトコル、たとえばDES等)、暗号化に使用される鍵(暗号鍵)、およびSPI(Security Parameter Index)のデータ項目を含んでいる。「SPI」は暗号化されたメッセージに付与され、受信側は、このSPIにより暗号プロトコルおよび鍵を特定し、受信したメッセージを復号化する。

#### 【0055】

加入者端末5の暗号処理管理部55は、SPDのIPアドレスおよびポート番号とそれぞれ一致するIPアドレスおよびポート番号を有するSAデータがSADに存在するかどうかを判断し、存在する場合には、その暗号化プロトコルおよび鍵を使用してメッセージを暗号化して送信し、存在しない場合には、存在しない旨をプロトコル制御部54に通知する。

#### 【0056】

図6は、鍵交換代理サーバ2の構成を示すブロック図である。鍵交換代理サーバ2は、メッセージ送受信部21、プロトコル制御部22、および鍵生成部23を有する。

#### 【0057】

メッセージ送受信部21は、コアネットワーク7に接続され、コアネットワーク7を介してサービス制御装置1からのメッセージを受信し、サービス制御装置1にメッセージを送信する。

#### 【0058】

プロトコル制御部 22 は、メッセージ送受信部 21 により受信されたメッセージの解析、通信相手端末 6 と鍵交換処理（鍵交換プロセス）を実行し、決定された鍵をメッセージ送受信部 21 に与える。

#### 【0059】

鍵生成部 23 は、プロトコル制御部 22 により実行される鍵交換プロセスにおいて、プロトコル制御部 22 の要求に応じて鍵を生成する。この鍵の生成において、たとえばべき乗計算が行われる。

#### 【0060】

次に、この鍵交換代理ネットワークシステムにおける鍵交換代理処理の流れを説明する。

#### 【0061】

図 7 は、加入者端末 5 による鍵交換メッセージ（鍵交換代理要求メッセージ）の送信から、加入者端末 5 と通信相手端末 6 との間で暗号化通信が行われるまでの全体のメッセージの流れを示している。図 8 は、加入者端末 5 の詳細な処理の流れを示すシーケンス図である。図 9 は、サービス制御装置 1 の詳細な処理の流れを示すシーケンス図である。図 10 は、図 9 のステップ S12 の詳細な処理の流れを示すフローチャートである。図 11 は、鍵交換代理サーバ 2 の詳細な処理の流れを示すシーケンス図である。

#### 【0062】

まず、図 8 を参照して、加入者端末 5 のメッセージ送受信部 52 は、アプリケーション処理部 51（図 8 には図示略）から与えられた通信相手端末 6 宛ての packets 送信要求（メッセージ送信要求）により、packets 送信を検出する（S1）。メッセージ送受信部 52 は、packets 送信を検出すると、packets の暗号化の必要の有無および鍵（暗号鍵）の有無を暗号処理管理部 55 に問い合わせる。

#### 【0063】

暗号処理管理部 55 は、メッセージ送受信部 52 の問合せにより、送信 packets の IP アドレス（宛先アドレス）およびポート番号とそれぞれ一致する IP アドレスおよびポート番号を有する IPSec 適用条件が SPD に存在するかどうかを判断する。一致する IPSec 適用条件が存在する場合には、暗号処理管理

部 5 5 は、送信パケットの暗号化が必要であると判断し、続いて、IP アドレスおよびポート番号とそれぞれ一致する SA データが SAD に存在するかどうかを判断する。一方、一致する IPSec 適用条件が存在しない場合には、暗号処理管理部 5 5 は上記処理を実行せず、送信パケットは通常の IP プロトコルに従って宛先アドレスが示す通信相手端末 6 に送信される。

#### 【 0 0 6 4 】

暗号化が必要であると判断された場合において、一致する SA データが SAD に存在しないときは、暗号処理管理部 5 5 は、鍵が存在しないことをプロトコル制御部 5 4 に通知する。この通知により、プロトコル制御部 5 4 は、鍵交換メッセージ（鍵交換代理要求メッセージ）を作成し、メッセージ送受信部 5 2 に与える。

#### 【 0 0 6 5 】

メッセージ送受信部 5 2 は、与えられた鍵交換メッセージをサービス制御装置 1（メッセージの宛先は通信相手端末 6）に送信する。この鍵交換メッセージの送信は、図 7 において符号（1）の破線の矢印で示される。

#### 【 0 0 6 6 】

なお、暗号化が必要であると判断された場合において、一致する SA データが SAD に存在するときの処理については、後の図 1 5 に従って説明する。

#### 【 0 0 6 7 】

図 1 2（A）は、加入者端末 5 からサービス制御装置 1 に送信される鍵交換メッセージ（鍵交換代理要求メッセージ）の構成を示している。この鍵交換メッセージは、IP ヘッダ（ヘッダ部）およびデータ部を有する。

#### 【 0 0 6 8 】

IP ヘッダには、送信元アドレス SA として加入者端末 5 の IP アドレスが、宛先アドレス DA として通信相手端末 6 の IP アドレスが、それぞれ含まれる。すなわち、加入者端末 5 は、あくまで通信相手端末 6 と通信を行うものと認識している。

#### 【 0 0 6 9 】

データ部には、UDP ヘッダおよび IKE ヘッダが含まれ、UDP ヘッダには

、 I P S e c / I K E における鍵交換メッセージで通常使用される U D P (User Datagram Protocol) の 5 0 0 番のポート番号が設定される。 I K E ヘッダにはクッキー (Cookie) が含まれ、このクッキーには特殊な値 (タイプ値) が設定される。特殊な値として、たとえば上位および下位の 8 バイトとも 1 0 0 が設定される。通常のメッセージでは、上位 8 バイトを送信者が決定し、下位 8 バイトを応答者が決定するために、この特殊な値を鍵交換代理サーバ 2 に予約しておくことにより、メッセージの識別が可能となる。なお、 U D P の値には、 5 0 0 番以外の値を使用することもできる。

#### 【 0 0 7 0 】

続いて、図 9 を参照して、サービス制御装置 1 のメッセージ送受信部 1 1 は、加入者端末 5 から鍵交換メッセージを受信すると、受信したメッセージをプロトコル制御部 1 2 に与える。

#### 【 0 0 7 1 】

プロトコル制御部 1 2 は、メッセージ送受信部 1 1 からメッセージを受け取ると、サービスプロファイル (図 3 参照) に基づいてメッセージ解析処理を実行する ( S 1 2 ) 。

#### 【 0 0 7 2 】

このメッセージ解析処理において、プロトコル制御部 1 2 は、図 1 0 に示すように、まず受信パケット (メッセージ) が加入者端末 5 から送信された鍵交換メッセージかどうかを判断する ( S 2 1 ) 。この判断は、受信パケットの送信元アドレス S A (すなわち加入者端末 5 の I P アドレス) と鍵交換メッセージに含まれるポート番号 (すなわち U D P の 5 0 0 番) とが、サービスプロファイルの I P S e c 適用条件に存在するかどうかと、受信パケットの内容に基づいて行われる。

#### 【 0 0 7 3 】

プロトコル制御部 1 2 は、送信元アドレスおよびポート番号がサービスプロファイルの I P S e c 適用条件に存在する場合には ( S 2 1 で Y ) 、受信パケットの内容に基づいて、その受信メッセージが鍵交換代理要求メッセージ、鍵交換メッセージ ( I K E メッセージ) 、または加入者端末 5 宛ての鍵情報 ( S A データ



)を含むメッセージ(鍵転送メッセージ)のいずれであるかを判断する。

#### 【0074】

たとえば、受信パケットにUDPヘッダやIKEヘッダが含まれている場合には、その受信パケットが鍵交換代理要求メッセージまたは鍵交換メッセージであると判断できる。鍵転送メッセージには、SAデータ等が含まれていることから、受信パケットが鍵転送メッセージであると判断できる。

#### 【0075】

そして、受信パケットが鍵交換代理要求メッセージである場合には(S21でY)、プロトコル制御部12は、メッセージ送受信部11を介して、受信パケット(すなわち鍵交換代理要求メッセージ)を鍵交換代理サーバ2に転送する(S26、図9のS13)。

#### 【0076】

受信パケットが鍵交換メッセージである場合には(S22でY)、プロトコル制御部12は、メッセージ送受信部11を介して、受信パケット(すなわち鍵交換メッセージ)を、その受信パケットの送信元アドレスまたは宛先アドレスに基づいて、鍵交換代理サーバ2または通信相手端末6に転送する(S26、図9のS13)。たとえば、受信パケットの送信元アドレスが通信相手端末6の場合には、受信パケットは鍵交換代理サーバ2に転送される。受信パケットの送信元アドレスが鍵交換代理サーバ2の場合には、受信パケットは通信相手端末6に転送される。

#### 【0077】

受信パケットが加入者宛ての鍵情報(SA)を含むメッセージである場合には(S23でY)、プロトコル制御部12は、メッセージ送受信部11を介して、受信パケットを加入者端末5に転送する(S25、図9のS13)。

#### 【0078】

受信パケットが鍵交換代理要求メッセージ、鍵交換メッセージ、および加入者宛ての鍵情報を含むメッセージのいずれでもない場合には(S21～S23でN)、プロトコル制御部12は通常のルーティングにしたがって受信パケットをルータ、端末等に転送する(S24、図9のS13)。

**【0079】**

このようにして、加入者端末5からサービス制御装置1に送信された鍵交換代理要求メッセージは、サービス制御装置1から鍵交換代理サーバ2に転送される。

**【0080】**

図12(B)は、サービス制御装置1から鍵交換代理サーバ2に転送される鍵交換代理要求メッセージの構成を示している。サービス制御装置1のプロトコル制御部12またはメッセージ送受信部11は、加入者端末5から送信された鍵交換代理要求メッセージをカプセル化し、新たなIPパケットのデータ部に組み込む。そして、この新たなIPパケットのIPヘッダには、送信元アドレスとしてサービス制御装置1のIPアドレスが書き込まれ、宛先アドレスとして鍵交換代理サーバ2のIPアドレスが書き込まれる。

**【0081】**

続いて、図11を参照して、鍵交換代理サーバ2のメッセージ送受信部21は、サービス制御装置1から、図12(B)に示す鍵交換代理要求メッセージを受信すると(S31)、受信メッセージをプロトコル制御部22に与える。

**【0082】**

プロトコル制御部22は、受信メッセージを解析し(S32)、受信メッセージが鍵交換代理要求メッセージであると判断すると、データ部にカプセル化された鍵交換代理要求メッセージの宛先アドレスDA(図12(B)参照)に基づいて通信相手(ここでは通信相手端末6)を特定する。そして、プロトコル制御部22は、特定した通信相手である通信相手端末6との間でIPSec/IKEに基づく鍵交換プロセスを実行する(S32)。この鍵交換プロセスにおいて、プロトコル制御部22は、必要に応じて鍵生成部23に鍵の生成を依頼し、この依頼に応じて、鍵生成部23は鍵を生成する。

**【0083】**

プロトコル制御部22は、鍵交換プロセスにおいて、通信相手端末6に送信する鍵交換メッセージ(IKEメッセージ)を作成する(S34)。図13(D)は、鍵交換代理サーバ2のプロトコル制御部22により作成される鍵交換メッセ

ージの構成を示している。

【0084】

鍵交換代理サーバ2は、加入者端末5の鍵交換処理を代理するものであるので、鍵交換代理サーバ2が作成する鍵交換メッセージのデータ部には、加入者端末5と通信相手端末6との間で交換される鍵交換メッセージ（IKEメッセージ）がカプセル化される。すなわち、データ部に含まれる鍵交換メッセージの送信元アドレスSAは加入者端末5のIPアドレスとなり、宛先アドレスDAは通信相手端末6のIPアドレスとなる。また、IPヘッダには、送信元アドレスSAとして鍵交換代理サーバ2のIPアドレスと、宛先アドレスDAとしてサービス制御装置1のIPアドレスが含まれる。なお、図13（D）に示す鍵交換メッセージのデータ部にカプセル化された鍵交換メッセージは、図12（A）に示す鍵交換メッセージ（鍵交換代理要求メッセージ）と同じ構造を有する。

【0085】

図11に戻って、図13（D）に示す鍵交換メッセージは、プロトコル制御部22からメッセージ送受信部21に与えられ、メッセージ送受信部21からサービス制御装置1に送信される（S35）。

【0086】

図9および図10を再び参照して、鍵交換代理サーバ2からサービス制御装置1に送信された鍵交換メッセージ（図13（D）参照）は、サービス制御装置1による前述した図10のステップS22およびS26の処理にしたがって通信相手端末6に転送される。この際、鍵交換代理サーバ2からサービス制御装置1に送信された鍵交換メッセージは、カプセル化が解除され、データ部にカプセル化された鍵交換メッセージが取り出される。図13（A）は、データ部から取り出されたメッセージの構成を示している。

【0087】

この取り出されたメッセージは、その宛先アドレスDA（すなわち通信相手端末6のIPアドレス）に基づいて、サービス制御装置1から通信相手端末6に送信される。

【0088】

通信相手端末 6 は、図 13 (A) に示す鍵交換メッセージを受信すると、鍵交換代理サーバ 2 と同様に IPsec/IKE による鍵交換プロセスを実行する。ここで、通信相手端末 6 が受信する鍵交換メッセージは図 13 (A) に示すものである。通信相手端末 6 は、鍵交換代理サーバ 2 ではなく、加入者端末 5 から鍵交換メッセージを受信したものと認識し、加入者端末 5 と鍵交換を行っていると判断する。

#### 【0089】

したがって、鍵交換プロセスにおいて通信相手端末 6 が送信する鍵交換メッセージは、図 13 (B) に示すように、送信元アドレス SA として通信相手端末 6 の IP アドレスを有し、宛先アドレス DA として加入者端末 5 の IP アドレスを有するメッセージとなる。

#### 【0090】

加入者端末 5 は、前述したように、サービス制御装置 1 と無線接続しているので、加入者端末 5 宛てに送信されるメッセージは、すべてサービス制御装置 1 を通過する。したがって、通信相手端末 6 から加入者端末 5 宛てに送信された鍵交換メッセージ (図 13 (B) 参照) は、サービス制御装置 1 に受信される。

#### 【0091】

サービス制御装置 1 は、前述した図 10 に示すステップ S22 および S26 の処理により、通信相手端末 6 から加入者端末 5 宛てに送信された鍵交換メッセージを鍵交換代理サーバ 2 に転送する。この際、この鍵交換メッセージは、図 13 (C) に示すようにカプセル化される。すなわち、通信相手端末 6 から送信された鍵交換メッセージがデータ部にカプセル化され、IP ヘッダの送信元アドレス SA はサービス制御装置 1 の IP アドレスとされ、宛先アドレス DA は鍵交換代理サーバ 2 の IP アドレスとされる。

#### 【0092】

図 11 に戻って、この図 13 (C) に示す鍵交換メッセージは、鍵交換代理サーバ 2 に受信され (S31)、メッセージ解析された後 (S32)、鍵交換プロセスに従って処理される (S33)。

#### 【0093】

このような処理が行われ、鍵交換代理サーバ 2 と通信相手端末 6 との間で鍵（暗号鍵）が決定される。このような鍵交換代理サーバ 2 と通信相手端末 6 との間における鍵交換メッセージの送受信は、図 7 の符号（2）の矢印で示される。

#### 【0 0 9 4】

鍵が決定されると、鍵交換代理サーバ 2 のプロトコル制御部 2 2 は、決定された鍵を鍵転送メッセージによりサービス制御装置 1 に送信する（S 3 4，S 3 5）。図 1 4（A）は、鍵交換代理サーバ 2 からサービス制御装置 1 に送信される鍵転送メッセージの構成を示している。

#### 【0 0 9 5】

この鍵転送メッセージの IP ヘッダには、送信元アドレスとして鍵交換代理サーバ 2 の IP アドレスが含まれ、宛先アドレスとしてサービス制御装置 1 の IP アドレスが含まれている。データ部には、鍵情報（SA データ）を含む鍵メッセージがカプセル化されている。

#### 【0 0 9 6】

鍵の交換は、鍵交換代理サーバ 2 が加入者端末 5 に代理して行っているものの、加入者端末 5 と通信相手端末 6 との間で行われたことになっている。したがって、カプセル化された鍵メッセージの IP ヘッダには、送信元アドレス SA として通信相手端末 6 の IP アドレスが含まれ、宛先アドレス DA として加入者端末 5 の IP アドレスが含まれる。

#### 【0 0 9 7】

鍵メッセージのデータ部には、鍵情報（すなわち図 5（B）に示す SA データ）が含まれている。

#### 【0 0 9 8】

鍵転送メッセージが鍵交換代理サーバ 2 からサービス制御装置 1 に送信されると、サービス制御装置 1 は、前述した図 1 0 のステップ S 2 3 および S 2 5 の処理により、鍵転送メッセージを加入者端末 5 に送信する。図 1 4（B）は、サービス制御装置 1 から加入者端末 5 に送信される鍵転送メッセージの構成を示している。

#### 【0 0 9 9】

この鍵転送メッセージは、前述した図 14 (A) に示すものとほぼ同じであるが、IPヘッダの送信元アドレス SA および宛先アドレス DA が異なる。送信元アドレス SA はサービス制御装置 1 の IP アドレスとされ、宛先アドレス DA は加入者端末 5 の IP アドレスとされる。

#### 【0100】

鍵交換代理サーバ 2 からサービス制御装置 1 を介して加入者端末 5 に送信される鍵転送メッセージの流れは、図 7 の符号 (3) の矢印により示される。

#### 【0101】

図 8 に戻って、加入者端末 5 のメッセージ送受信部 52 は、サービス制御装置 1 から鍵転送メッセージを受信すると (S5)、カプセル化を解除して、データ部に含まれる鍵メッセージをプロトコル制御部 54 に与える。

#### 【0102】

プロトコル制御部 54 は、鍵メッセージに含まれる鍵情報 (SA データ) を抽出し、SA データを暗号処理管理部 55 に与える (S6)。暗号処理管理部 55 は、プロトコル制御部 54 から受け取った SA データを SAD に追加する (S7)。

#### 【0103】

以後、加入者端末 5 は、この SA データに含まれる鍵および暗号化プロトコルに従ってデータを暗号化し、暗号化されたデータを通信相手端末 6 に送信する。図 15 は、鍵が決定された後の加入者端末 5 のパケットの送受信処理の流れを示すシーケンス図である。

#### 【0104】

加入者端末 5 のアプリケーション処理部 51 が通信相手端末 6 宛てのパケット送信要求をメッセージ送受信部 52 に与えると、メッセージ送受信部 52 は、パケット送信を検出し (S41)、パケットの暗号化の必要の有無および鍵の有無を暗号処理管理部 55 に問い合わせる。暗号処理管理部 55 は、SPD および SAD (図 5 (A) および (B) 参照) により暗号化の必要の有無および鍵の有無を判断する (S42)。これらの処理は、前述した図 8 のステップ S1 および S2 の処理と同じである。

**【0 1 0 5】**

ここでは、暗号化が必要であり、かつ、鍵が存在するものとする。この場合に、暗号処理管理部 5 5 は、S P D の I P アドレスおよびポート番号にそれぞれ一致する I P アドレスおよびポート番号を有する S A データを選択し（S 4 3）、選択した S A データに基づく暗号化処理を暗号化／復号化部 5 3 に指示する。

**【0 1 0 6】**

暗号化／復号化部 5 3 は、この指示により、選択された S A データの鍵および暗号化プロトコルを使用してパケットを暗号化する（S 4 4）。また、暗号化／復号化部 5 3 は、選択された S A データに含まれる S P I を暗号化されたパケットの所定のフィールドに書き込む。

**【0 1 0 7】**

この暗号化されたパケットは、メッセージ送受信部 5 2 に与えられ、メッセージ送受信部 5 2 からサービス制御装置 1 に送信される（S 4 5）。サービス制御装置 1 は、このパケットを図 1 0 のステップ S 2 4 の通常ルーティング処理により転送する。これにより、このパケットは、サービス制御装置 1 からルータ 4 を介して通信相手端末 6 に送信される。このパケットの送信は、図 7 の符号（4）の矢印により示される。

**【0 1 0 8】**

通信相手端末 6 は、暗号化されたパケットを受信すると、パケットに含まれる S P I および保持する S A D に基づいて、鍵および暗号化プロトコルを特定し、特定した鍵および暗号化プロトコルに基づいてパケットを復号化する。

**【0 1 0 9】**

一方、通信相手端末 6 から加入者端末 5 に暗号化パケットが送信されると、この暗号化パケットは、ルータ 4 およびサービス制御装置 1 を介して加入者端末 5 のメッセージ送受信部 5 2 に受信される（S 4 6）。このパケットの送信も、図 7 の符号（4）の矢印により示される。

**【0 1 1 0】**

メッセージ送受信部 5 2 は、受信したパケットを暗号化／復号化部 5 3 に与える。暗号化／復号化部 5 3 は、パケットに含まれる S P I を暗号処理管理部 5 5

に与える。暗号処理管理部 55 は、暗号化／復号化部 53 から与えられた S P I と一致する S A データを S A D から検索および抽出し (S 47) , 抽出した S A データの鍵および暗号化プロトコル (復号化プロトコル) を暗号化／復号化部 53 に与える。

#### 【0111】

暗号化／復号化部 53 は、暗号処理管理部 55 から与えられた鍵および暗号化プロトコルに従ってパケットを復号化する (S 48) 。

#### 【0112】

このようにして、加入者端末 5 と通信相手端末 6 との間で、暗号化通信が行われる。

#### 【0113】

次に、通信相手端末 6 から加入者端末 5 宛てに、I P S e c / I K E に基づく鍵交換要求が送信された場合の処理について説明する。

#### 【0114】

図 16 は、通信相手端末 6 による鍵交換メッセージの送信から、通信相手端末 6 と加入者端末 5 との間で暗号化通信が行われるまでの全体のメッセージの流れを示している。

#### 【0115】

通信相手端末 6 においても、加入者端末 5 と同様にして、加入者端末 5 宛てのパケットの暗号化の必要の有無および鍵の有無が S P D および S A D に基づいて判断される。そして、暗号化が必要と判断されたが、鍵 (および暗号化プロトコル) を規定した S A データが存在しない場合には、通信相手端末 6 は、前述した図 13 (B) に示す鍵交換メッセージを加入者端末 5 宛てに送信する。

#### 【0116】

この鍵交換メッセージは、その宛先アドレス D A が加入者端末 5 の I P アドレスであるので、サービス制御装置 1 に受信される。サービス制御装置 1 は、図 10 のステップ S 22 および S 26 の処理に従って、鍵交換メッセージを図 13 (C) に示すようにカプセル化し、カプセル化後の鍵交換メッセージを鍵交換代理サーバ 2 に転送する。この鍵交換メッセージの流れが図 16 の符号 (1) の矢印



で示されている。

#### 【0117】

その後、前述と同様にして、鍵交換代理サーバ2と通信相手端末6との間で、鍵交換プロセスに従って鍵交換メッセージが交換され、鍵が決定される。この鍵交換メッセージの交換は、図16の符号(2)の矢印で示されている。

#### 【0118】

鍵交換代理サーバ2と通信相手端末6との間で鍵が決定されると、決定された鍵は、図14(A)に示す鍵転送メッセージとして鍵交換代理サーバ2からサービス制御装置1に送信され、さらに、図14(B)に示す鍵転送メッセージとしてサービス制御装置1から加入者端末5に送信される。この鍵転送メッセージの流れが図16の符号(3)の矢印で示されている。

#### 【0119】

加入者端末5は、鍵転送メッセージを受信すると、前述したのと同様に、鍵転送メッセージに含まれるSAデータをSADに追加する。その後、加入者端末5は、通信相手端末6から送信されてきた暗号化パケットをSADに基づいて復号化し、また、通信相手端末6宛てに送信するパケットをSADに基づいて暗号化して送信する。この通信相手端末6と加入者端末5との間の暗号化パケットの送受信が図16の符号(4)の矢印で示されている。

#### 【0120】

このように、本発明の実施の形態によると、IPSec/IKEに基づく鍵交換処理を、鍵交換代理サーバ2が加入者端末5に代わって通信相手端末6との間で実行する。したがって、加入者端末5がIPSec/IKEによる鍵交換処理を行う必要はないので、加入者端末5の処理が軽減される。また、加入者端末5は鍵交換処理のプログラム(鍵交換サーバ)を保持する必要はないので、加入者端末5のメモリ容量を小さくすることができ、その結果、装置の小型軽量化および装置コストの低減を図ることができる。さらに、鍵交換サーバの実行に伴う電力消費もないので、加入者端末5の省電力化に貢献する。

#### 【0121】

また、本発明の実施の形態によると、サービス制御装置1が、鍵交換代理サー

バ2の位置（IPアドレス）を知り、サービスプロファイルに基づいて鍵交換代理サーバ2へのメッセージ転送の必要の有無を判断する。したがって、加入者端末5および通信相手端末6は、ともに鍵交換代理サーバ2の位置を知る必要はなく、知らなくても鍵交換を行い、その後の暗号化通信を行うことができる。

#### 【0122】

なお、通信相手端末6も、加入者端末5と同様に、鍵交換サーバを有しない携帯端末等の場合もある。この場合には、通信相手端末6がアクセスするルータ4がサービス制御装置となり、また、このサービス制御装置の最寄りの鍵交換代理サーバが通信相手端末6に代わって鍵交換処理を行う。そして、加入者端末5の鍵交換代理サーバ2と通信相手端末6の鍵交換代理サーバとの間で鍵交換処理が実行され、決定された鍵が、それぞれの鍵交換代理サーバから加入者端末5および通信相手端末6にそれぞれ送信される。

#### 【0123】

また、このように、通信相手端末6について、鍵交換代理サーバが鍵交換を代行する場合に、この鍵交換代理サーバは、加入者端末5の鍵交換を代行する鍵交換代理サーバと同一のサーバであってもよい。同様にして、通信相手端末6のメッセージ転送を行うサービス制御装置も、サービス制御装置1と同一であってもよい。

#### 【0124】

コアネットワーク7の運用者には、特定のアクセス手段を所有せず、大規模ネットワークの運用者からネットワーク（の一部）を借りて、利用者にサービスを提供するMNVO（Mobile Virtual Network Operator）も含まれる。

#### 【0125】

（付記1） 暗号通信を行う第1および第2の端末装置の間で行われる鍵交換処理を代行する鍵交換代理ネットワークシステムであって、

前記第1の端末装置にアクセスされる第1のサービス制御装置および前記第1の端末装置の鍵交換処理を代行する第1の鍵交換代理装置を備え、

前記第1のサービス制御装置は、

前記第1もしくは第2の端末装置または前記第1の鍵交換代理装置からのメッ

セージを受信する第 1 のメッセージ受信部と、

前記第 1 のメッセージ受信部により受信されたメッセージが鍵交換メッセージまたは鍵を含むメッセージかどうかを判断するための第 1 のデータを保持し、該第 1 のデータに基づいて前記受信メッセージが前記鍵交換メッセージまたは前記鍵を含むメッセージかどうかを判断し、前記受信メッセージが前記第 1 または第 2 の端末装置からの鍵交換メッセージの場合には転送先を前記第 1 の鍵交換代理装置とし、前記受信メッセージが前記第 1 の鍵交換代理装置からの鍵交換メッセージの場合には転送先を前記第 2 の端末装置とし、前記受信メッセージが前記鍵を含むメッセージの場合には転送先を前記第 1 の端末装置として決定する第 1 のプロトコル制御部と、

前記第 1 のプロトコル制御部により決定された転送先に前記第 1 のメッセージ受信部により受信されたメッセージを送信する第 1 のメッセージ送信部と、

を備え、

前記第 1 の鍵交換代理装置は、

前記第 1 のサービス制御装置からのメッセージを受信する第 2 のメッセージ受信部と、

前記第 2 のメッセージ受信部により受信されたメッセージが前記鍵交換メッセージである場合に、前記第 2 の端末装置との間で前記鍵交換メッセージを交換して鍵を決定する第 2 のプロトコル制御部と、

前記第 2 のプロトコル制御部により決定された前記鍵を、前記鍵を含むメッセージとして前記第 1 のサービス制御装置宛てに送信する第 2 のメッセージ送信部と、

を備えている鍵交換代理ネットワークシステム。

#### 【0 1 2 6】

(付記 2) 付記 1 において、

前記第 2 のプロトコル制御部は、前記第 1 の端末装置からの鍵交換メッセージの受信を契機として前記第 2 の端末装置との間で鍵を決定する、鍵交換ネットワークシステム。

#### 【0 1 2 7】

(付記 3) 付記 1 において、

前記第 2 のプロトコル制御部は、前記第 2 の端末装置からの鍵交換メッセージの受信を契機として前記第 2 の端末装置との間で鍵を決定する、鍵交換ネットワークシステム。

【 0 1 2 8 】

(付記 4) 付記 1 から 3 のいずれか 1 つにおいて、

前記第 2 の端末装置にアクセスされる第 2 のサービス制御装置および前記第 2 の端末装置の鍵交換処理を代行する第 2 の鍵交換代理装置をさらに備え、

前記第 2 のサービス制御装置は、

前記第 1 もしくは第 2 の端末装置または前記第 2 の鍵交換代理装置からのメッセージを受信する第 3 のメッセージ受信部と、

前記第 3 のメッセージ受信部により受信されたメッセージが鍵交換メッセージまたは鍵を含むメッセージかどうかを判断するための第 2 のデータを保持し、該第 2 のデータに基づいて前記受信メッセージが前記鍵交換メッセージまたは前記鍵を含むメッセージかどうかを判断し、前記受信メッセージが前記第 1 または第 2 の端末装置からの鍵交換メッセージの場合には転送先を前記第 2 の鍵交換代理装置とし、前記受信メッセージが前記第 2 の鍵交換代理装置からの鍵交換メッセージの場合には転送先を前記第 1 の端末装置とし、前記受信メッセージが前記鍵を含むメッセージの場合には転送先を前記第 2 の端末装置として決定する第 3 のプロトコル制御部と、

前記第 3 のプロトコル制御部により決定された転送先に前記第 3 のメッセージ受信部により受信されたメッセージを送信する第 3 のメッセージ送信部と、

を備え、

前記第 2 の鍵交換代理装置は、

前記第 2 のサービス制御装置からのメッセージを受信する第 4 のメッセージ受信部と、

前記第 4 のメッセージ受信部により受信されたメッセージが前記鍵交換メッセージである場合に、前記第 1 の鍵交換代理装置との間で前記鍵交換メッセージを交換して鍵を決定する第 4 のプロトコル制御部と、

前記第4の Protokol 制御部により決定された前記鍵を、前記鍵を含むメッセージとして前記第2のサービス制御装置宛てに送信する第4のメッセージ送信部と、

を備えている鍵交換代理ネットワークシステム。

#### 【0129】

(付記5) 付記4において、

前記第1および第2のサービス制御装置が同一の装置により構成される、鍵交換代理ネットワークシステム。

#### 【0130】

(付記6) 付記4または5において、

前記第1および第2の鍵交換代理装置が同一の装置により構成される、鍵交換代理ネットワークシステム。

#### 【0131】

(付記7) 端末装置によりアクセスされ、該端末装置、該端末装置の鍵交換処理を代行する鍵交換代理装置、または該端末装置と暗号通信を行う通信相手端末からのメッセージを転送するサービス制御装置であって、

前記端末装置、前記鍵交換代理装置、または前記通信相手端末装置からのメッセージを受信するメッセージ受信部と、

前記メッセージ受信部により受信されたメッセージが鍵交換メッセージまたは鍵を含むメッセージかどうかを判断するためのデータを保持し、該データに基づいて前記受信メッセージが前記鍵交換メッセージまたは前記鍵を含むメッセージかどうかを判断し、前記受信メッセージが前記端末装置または通信相手端末装置からの鍵交換メッセージの場合には転送先を前記鍵交換代理装置とし、前記受信メッセージが前記鍵交換代理装置からの鍵交換メッセージの場合には転送先を前記通信相手端末装置とし、前記受信メッセージが前記鍵を含むメッセージの場合には転送先を前記端末装置として決定する Protokol 制御部と、

前記 Protokol 制御部により決定された転送先に前記受信メッセージを送信するメッセージ送信部と、

を備えているサービス制御装置。

**【 0 1 3 2 】**

(付記 8) 付記 7 において、

前記データは、端末装置ごとに設けられ、アドレスとアプリケーションを指定するポート番号とを含むサービスプロファイルであり、

前記プロトコル制御部は、前記メッセージ受信部により受信されたメッセージの宛先アドレスまたは送信元アドレスと前記サービスプロファイルのアドレス、および、前記受信メッセージに含まれるポート番号と前記サービスプロファイルのポート番号を比較することにより、前記受信メッセージが前記鍵交換メッセージまたは前記鍵を含むメッセージかどうかを判断する、

サービス制御装置。

**【 0 1 3 3 】**

(付記 9) 通信相手端末装置と暗号通信を行う端末装置に代わって前記通信相手端末との間で鍵交換処理を行う鍵交換代理装置であって、

前記端末装置にアクセスされ、前記端末装置または前記通信相手端末装置からのメッセージを転送するサービス制御装置からのメッセージを受信するメッセージ受信部と、

前記メッセージ受信部により受信されたメッセージが鍵交換メッセージである場合に、前記通信相手端末装置との間で前記鍵交換メッセージを交換して鍵を決定するプロトコル制御部と、

前記プロトコル制御部により決定された前記鍵を、前記鍵を含むメッセージとして前記サービス制御装置宛てに送信するメッセージ送信部と、

を備えている鍵交換代理装置。

**【 0 1 3 4 】**

(付記 1 0) 付記 9 において、

前記鍵を生成する鍵生成部をさらに備えている鍵交換代理装置。

**【 0 1 3 5 】**

(付記 1 1) 付記 9 または 1 0 において、

前記プロトコル制御部は、前記端末装置からの鍵交換メッセージの受信を契機として前記通信相手端末装置との間で鍵を決定する、鍵交換代理装置。

**【 0 1 3 6 】**

(付記 1 2) 付記 9 または 1 0 において、

前記プロトコル制御部は、前記通信相手端末装置からの鍵交換メッセージの受信を契機として前記通信相手端末装置との間で鍵を決定する、鍵交換代理装置。

**【 0 1 3 7 】**

(付記 1 3) 通信ネットワークのサービス制御装置にアクセスして、通信相手端末装置と暗号通信を行う端末装置であって、

暗号化が必要な通信の条件を規定した第 1 のデータおよび暗号化に使用される鍵を含む第 2 のデータを保持し、前記第 1 のデータに基づいて通信相手端末装置との通信に暗号化が必要かどうかを判断し、暗号化に必要な鍵が前記第 2 のデータに存在するかどうかを判断する暗号処理管理部と、

前記暗号処理管理部により暗号化が必要であると判断され、かつ、暗号化に必要な鍵が存在しないと判断された場合に、鍵交換メッセージを前記サービス制御装置を介して前記通信相手端末宛てに送信するメッセージ送信部と、

前記通信ネットワークの鍵交換代理装置と前記通信相手端末装置との間で決定された鍵を含むメッセージを前記サービス制御装置から受信するメッセージ受信部と、

を備えている端末装置。

**【 0 1 3 8 】**

(付記 1 4) 付記 1 3 において、

前記第 1 のデータは、暗号化通信が必要な通信相手端末のアドレスと、アプリケーションを指定するポート番号とを含み、

前記暗号処理管理部は、前記通信相手端末装置に送信するメッセージの宛先アドレスと前記第 1 のデータのアドレス、および、前記送信メッセージに含まれるポート番号と前記第 1 のデータのポート番号を比較することにより、前記通信相手端末との通信に暗号化が必要かどうかを判断する、

端末装置。

**【 0 1 3 9 】**

(付記 1 5) 付記 1 3 または 1 4 において、

前記第 2 のデータは、アドレスおよびポート番号、ならびに、暗号化プロトコルおよび暗号化に使用される鍵を含み、

前記暗号処理管理部は、前記第 1 のデータアドレスと前記第 2 のデータのアドレス、および、前記第 1 のデータのポート番号と前記第 1 のデータのポート番号を比較することにより、暗号化に必要な鍵が前記第 2 のデータに存在するかどうかを判断する

端末装置。

#### 【0 1 4 0】

(付記 1 6) 暗号通信を行う第 1 および第 2 の端末装置の間で行われる鍵交換処理を前記第 1 の端末装置に代わって行う鍵交換代理装置および前記第 1 の端末装置にアクセスされるサービス制御装置を有する鍵交換代理ネットワークシステムで実行される鍵交換代理方法であって、

前記サービス制御装置において、前記第 1 または第 2 の端末装置から送信される鍵交換メッセージを前記鍵交換代理装置に転送し、

前記鍵交換代理装置において、前記第 1 の端末装置と前記第 2 の端末装置との間で交換される鍵交換メッセージを作成して前記サービス制御装置に送信し、

前記サービス制御装置において、前記鍵交換メッセージを前記第 2 の端末装置に転送し、

前記鍵交換代理装置において、前記鍵交換メッセージの交換により決定された鍵を含むメッセージを前記サービス制御装置に送信し、

前記サービス制御装置において、前記鍵交換代理装置から送信された前記鍵を含むメッセージを前記第 1 の端末装置に転送する、

鍵交換代理方法。

#### 【0 1 4 1】

(付記 1 7) 暗号通信を行う第 1 および第 2 の端末装置の間で行われる鍵交換処理を代行する鍵交換代理ネットワークシステムであって、

前記第 1 の端末装置にアクセスされるサービス制御装置および前記第 1 の端末装置の鍵交換処理を代行する鍵交換代理装置を備え、

前記サービス制御装置は、受信メッセージの転送先を判断するためのサービス



プロファイルに基づいて、前記第 1 の端末装置からの鍵交換代理要求メッセージまたは前記第 2 の端末装置からの鍵交換メッセージを前記鍵交換代理装置に転送し、前記鍵交換代理装置からの鍵交換メッセージを前記第 2 の端末装置に転送するとともに、前記鍵交換代理装置からの鍵を含むメッセージを前記第 1 の端末装置に転送し、

前記鍵交換代理装置は、前記鍵交換メッセージを前記第 2 の端末装置との間で前記サービス制御装置を介して交換して鍵を決定し、決定した鍵を含むメッセージを前記サービス制御装置を介して前記第 1 の端末装置に送信する、

鍵交換代理ネットワークシステム。

#### 【0142】

#### 【発明の効果】

本発明によると、端末装置は、鍵交換および鍵決定に必要な処理を行うことなく、暗号通信に必要な鍵を得ることができ、端末装置の負荷が軽減される。また、端末装置およびその通信相手端末装置のいずれから鍵交換処理の要求があっても、ネットワークシステムの鍵交換代理装置（鍵交換代理サーバ）による鍵交換処理の代行が可能である。

#### 【図面の簡単な説明】

#### 【図 1】

本発明の実施の形態による鍵交換代理ネットワークシステムの構成を示すブロック図である。

#### 【図 2】

サービス制御装置の構成を示すブロック図である。

#### 【図 3】

サービスプロファイルの一例を示す。

#### 【図 4】

加入者端末の構成を示すブロック図である。

#### 【図 5】

(A) は、加入者端末の暗号処理管理部に保持される SPD を示し、(B) は加入者端末の暗号処理管理部に保持される SAD を示している。

**【図 6】**

鍵交換代理サーバの構成を示すブロック図である。

**【図 7】**

加入者端末による鍵交換代理要求メッセージの送信から、加入者端末と通信相手端末との間で暗号化通信が行われるまでの全体のメッセージの流れを示す。

**【図 8】**

加入者端末の詳細な処理の流れを示すシーケンス図である。

**【図 9】**

サービス制御装置に詳細な処理の流れを示すシーケンス図である。

**【図 1 0】**

図 9 のステップ S 1 2 の詳細な処理の流れを示すフローチャートである。

**【図 1 1】**

鍵交換代理サーバの詳細な処理の流れを示すシーケンス図である。

**【図 1 2】**

(A) は、加入者端末からサービス制御装置に送信される鍵交換代理要求メッセージの構成を示し、

**【図 1 3】**

(A) はサービス制御装置から通信相手端末に送信される鍵交換メッセージを、(B) は通信相手端末からサービス制御装置に送信される鍵交換メッセージを、(C) はサービス制御装置から鍵交換代理サーバに送信される鍵交換メッセージを、(D) は鍵交換代理サーバからサービス制御装置に送信される鍵交換メッセージを、それぞれ示す。

**【図 1 4】**

(A) は、鍵交換代理サーバからサービス制御装置に送信される鍵転送メッセージの構成を示し、(B) は、サービス制御装置から加入者端末に送信される鍵転送メッセージを示す。

**【図 1 5】**

鍵が決定された後の加入者端末 5 のパケットの送受信処理の流れを示すシーケンス図である。

**【図 1 6】**

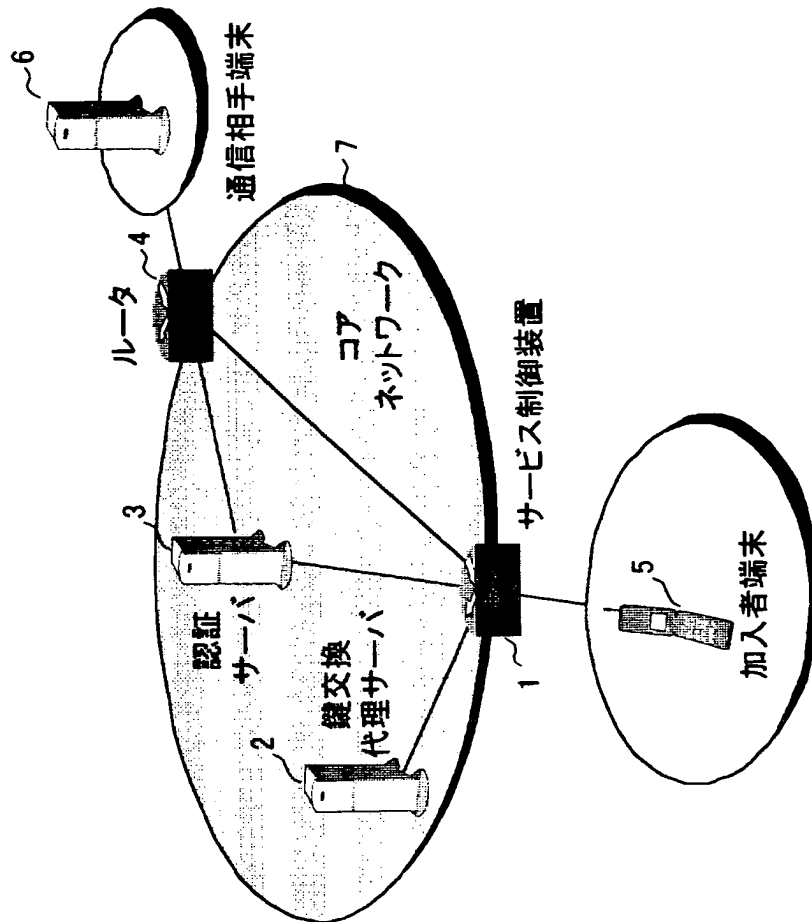
通信相手端末による鍵交換メッセージの送信から，通信相手端末と加入者端末との間で暗号化通信が行われるまでの全体のメッセージの流れを示す。

**【符号の説明】**

- 1 サービス制御装置
- 2 鍵交換代理サーバ
- 3 認証サーバ
- 5 加入者端末
- 6 通信相手端末
- 7 コアネットワーク
- 1 1， 2 1， 5 2 メッセージ送受信部
- 1 2， 2 2， 5 4 プロトコル制御部
- 2 3 鍵生成部
- 5 3 暗号化／復号化部
- 5 5 暗号処理管理部

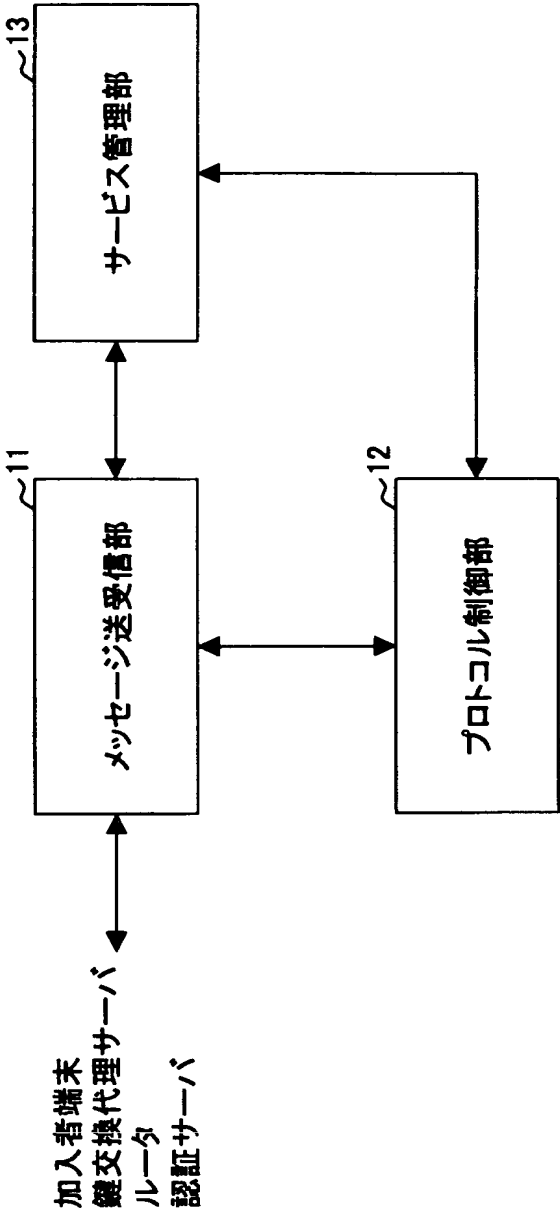
【書類名】 図面

【図 1】



【図 2】

サービス制御装置の構成



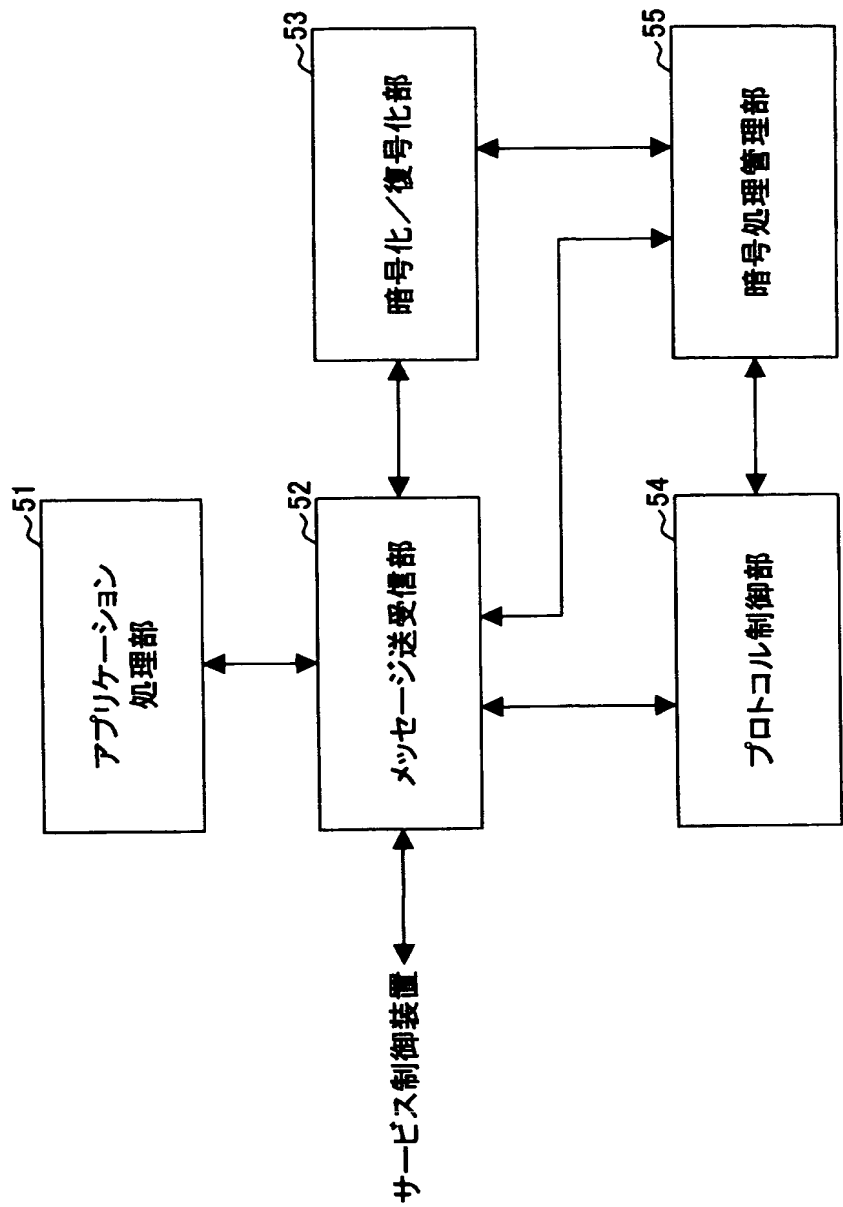
【図 3】

## サービスプロファイル

名称	内容
加入者識別情報	電話番号
	NAI
	認証データベースのエントリ番号
	・ ・ ・
IPSec適用条件1	IPアドレス
	ポート番号
IPSec適用条件2	IPアドレス
	ポート番号
・ ・ ・	・ ・ ・

【図 4】

加入者端末の構成



【図 5】

## 加入者端末の保持データ

## (A) SPD

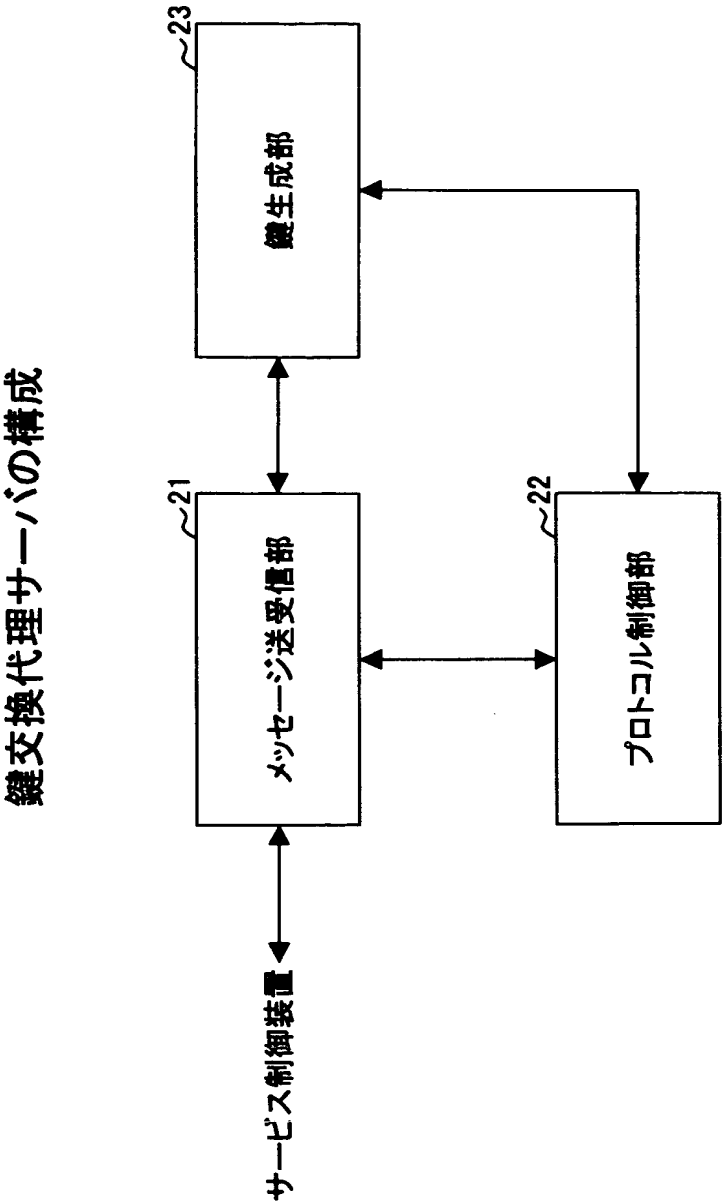
名称	内容
IPSec適用条件1	IPアドレス
	ポート番号
IPSec適用条件2	IPアドレス
	ポート番号
⋮	⋮

## (B) SAD

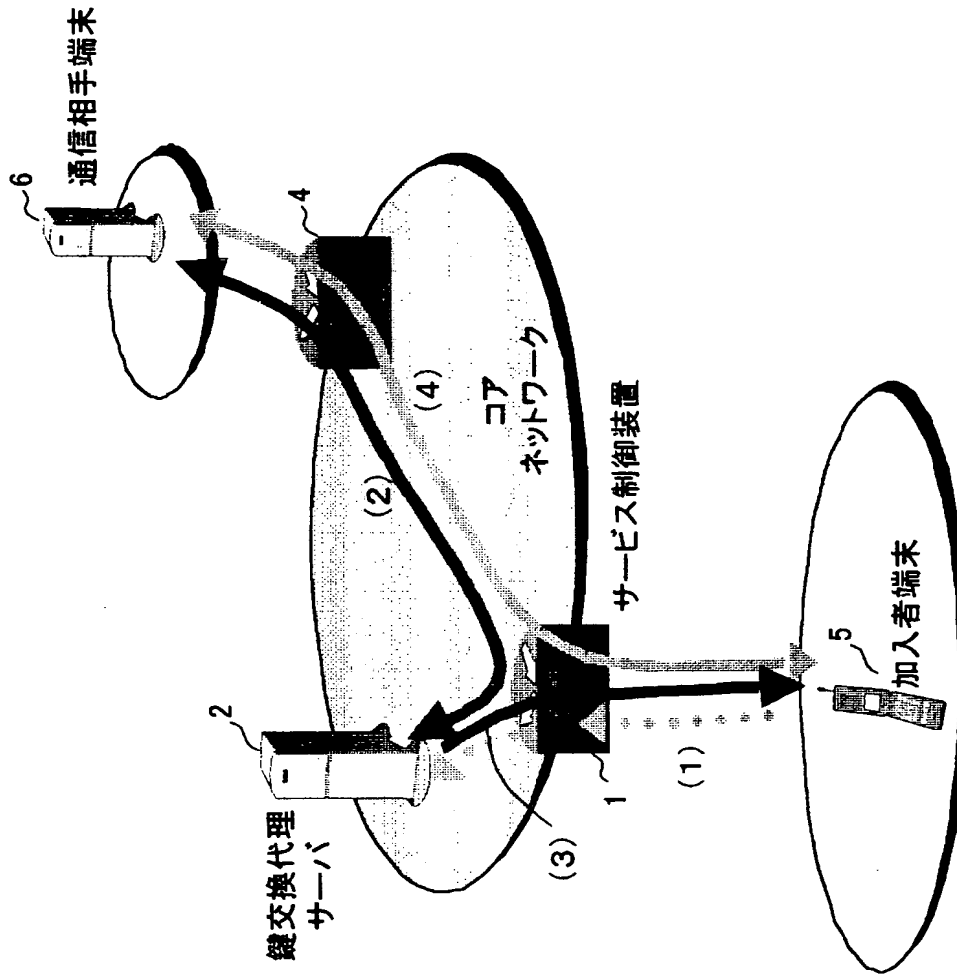
名称	適用条件	内容
IPSec適用条件1	IPアドレス	暗号化プロトコル
	ポート番号	鍵
IPSec適用条件2	IPアドレス	SPI
	ポート番号	暗号化プロトコル
⋮	⋮	鍵
⋮	⋮	SPI
⋮	⋮	⋮



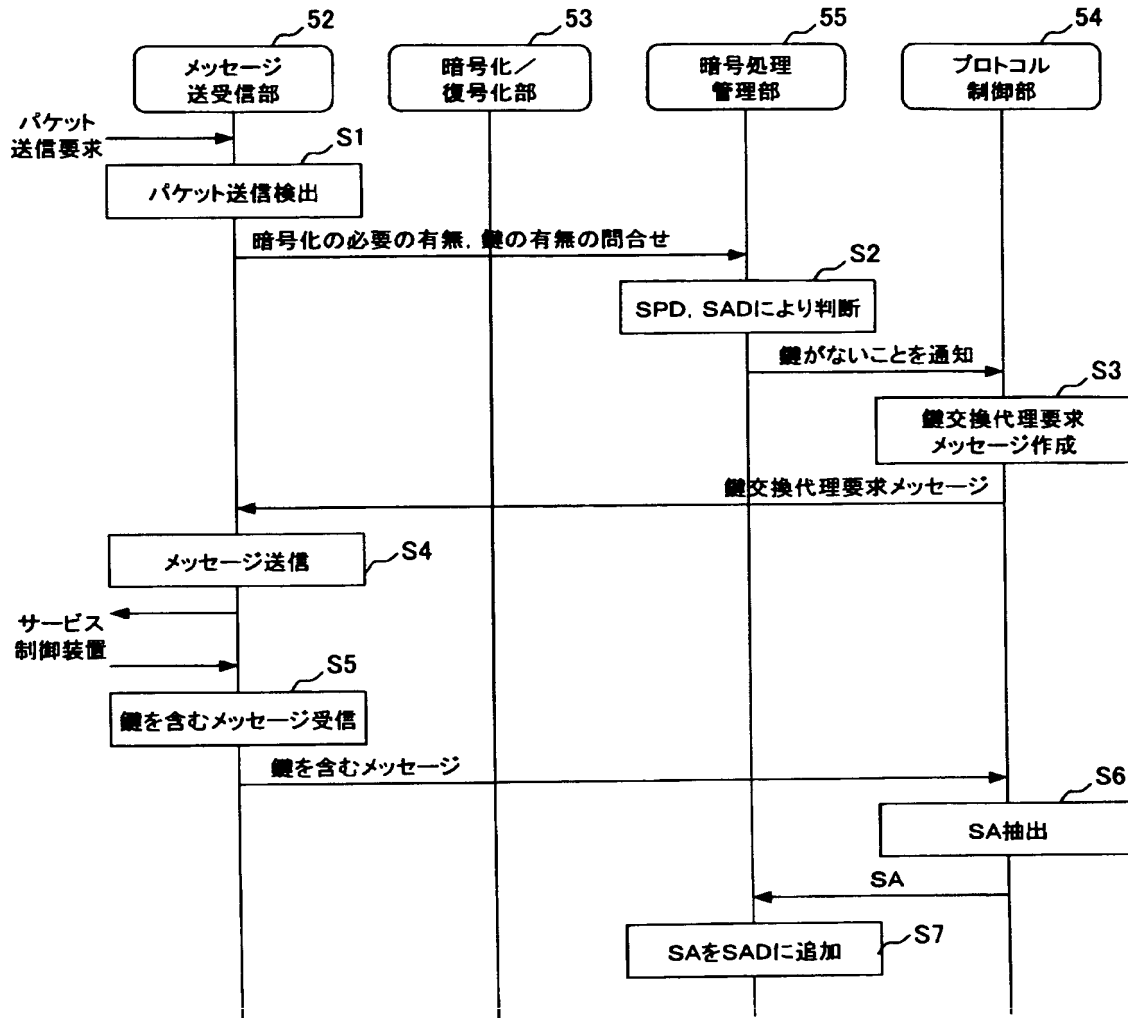
【図 6】



【図 7】

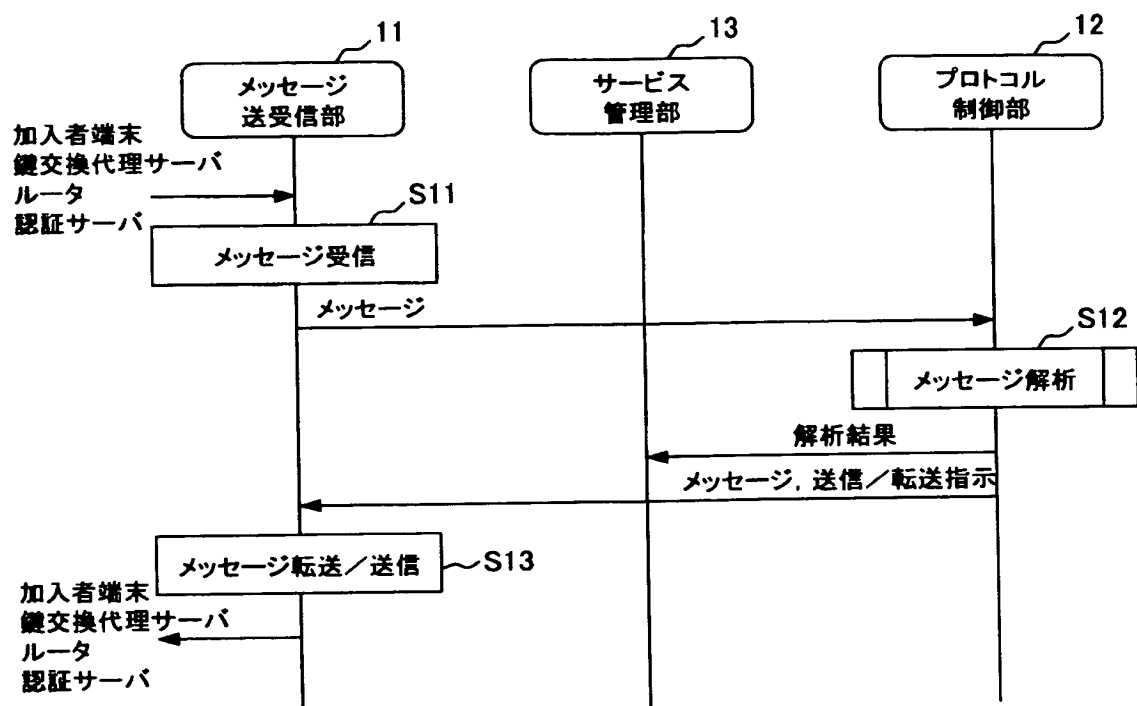


【図 8】

加入者端末の処理シーケンス  
(加入者端末からの通信開始時)

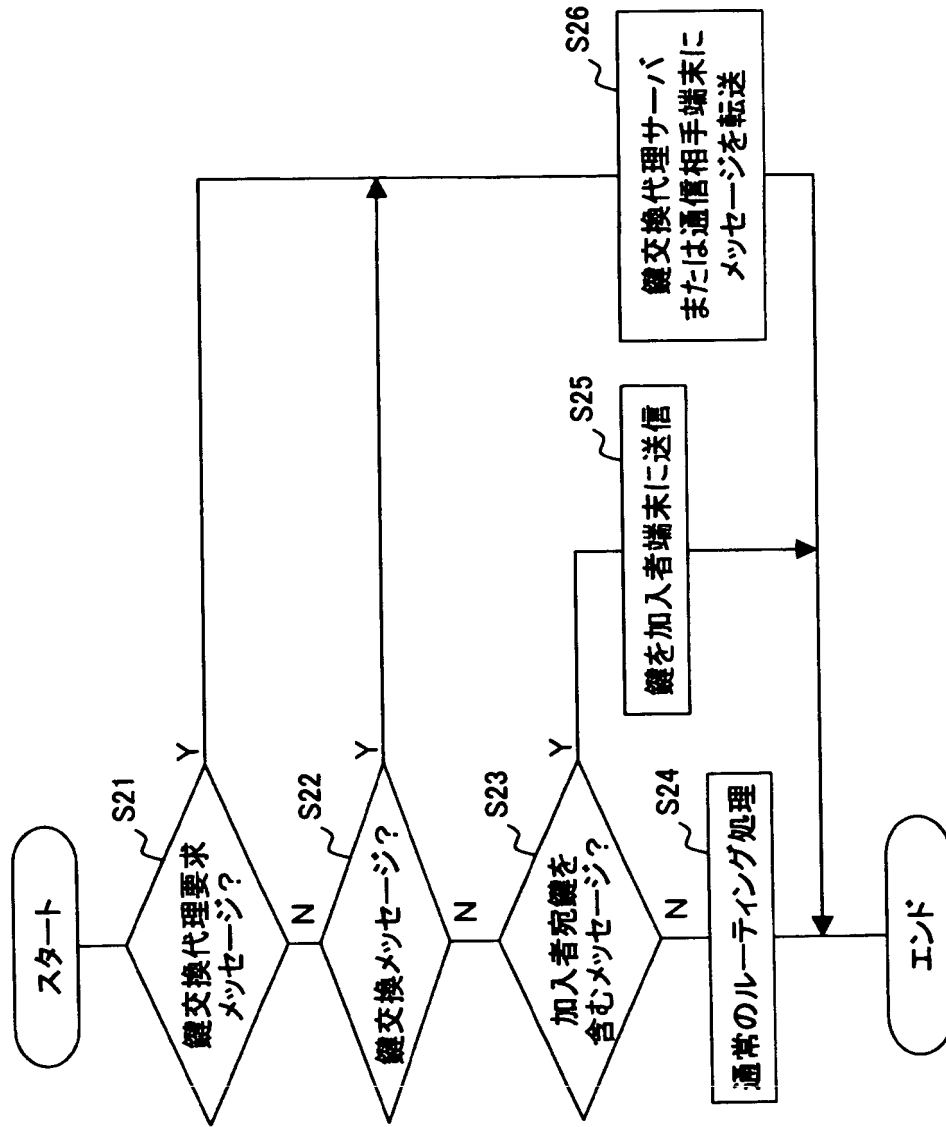
【図 9】

## サービス制御装置の処理シーケンス



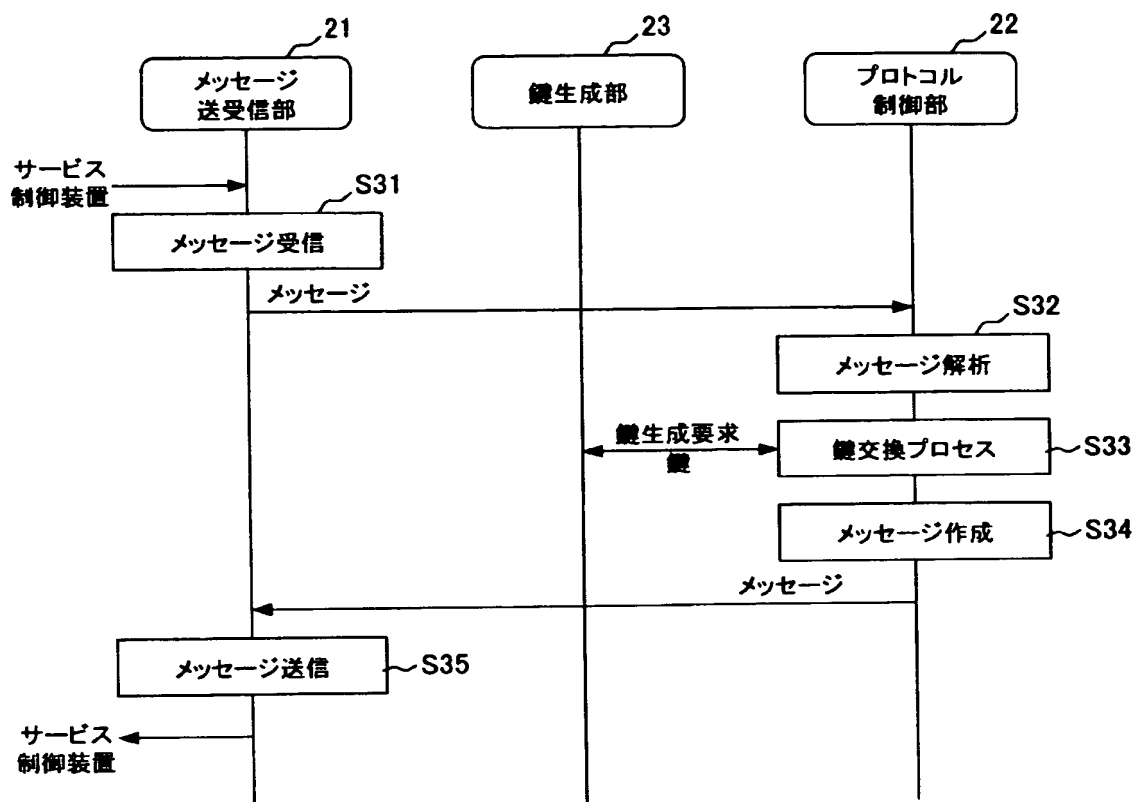
【図 10】

## サービス制御装置のメッセージ解析処理フロー



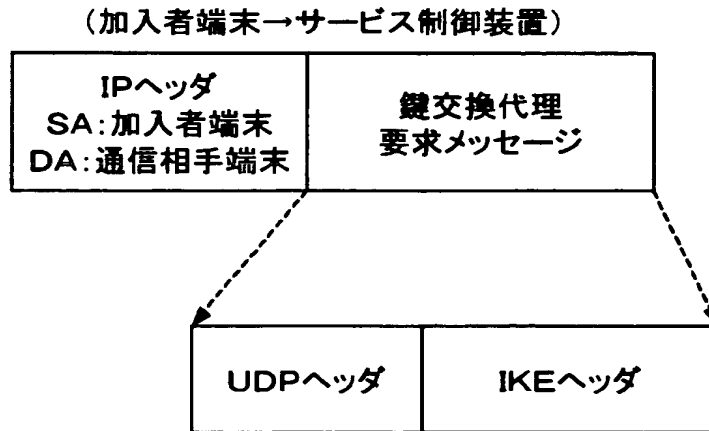
【図 11】

## 鍵交換代理サーバの処理シーケンス

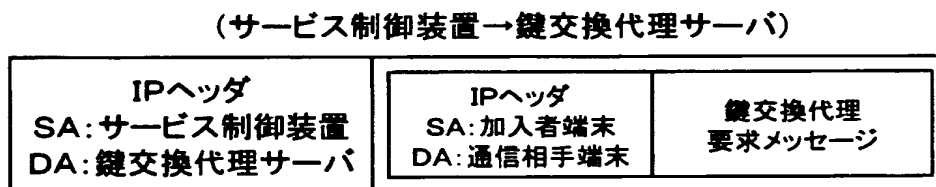


【図 12】

## (A) 鍵交換メッセージ(鍵交換代理要求メッセージ)



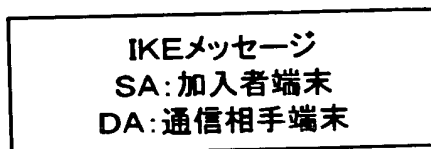
## (B) 鍵交換メッセージ(鍵交換代理要求メッセージ)



【図 13】

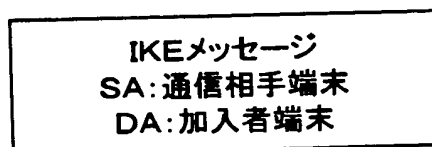
## (A) 鍵交換メッセージ

(サービス制御装置→通信相手端末)



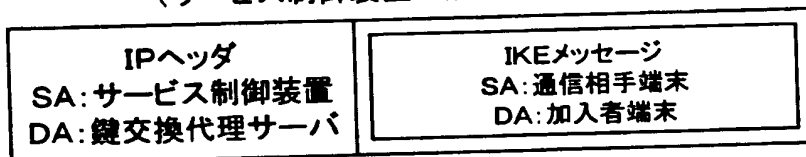
## (B) 鍵交換メッセージ

(通信相手端末→サービス制御装置)



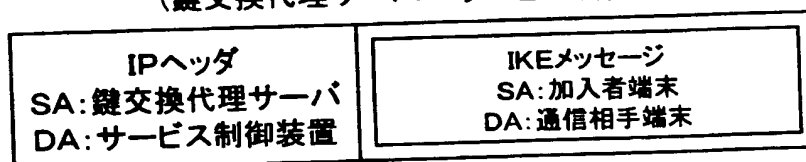
## (C) 鍵交換メッセージ

(サービス制御装置→鍵交換代理サーバ)



## (D) 鍵交換メッセージ

(鍵交換代理サーバ→サービス制御装置)





【図 14】

## (A) 鍵転送メッセージ

(鍵交換代理サーバ→サービス制御装置)

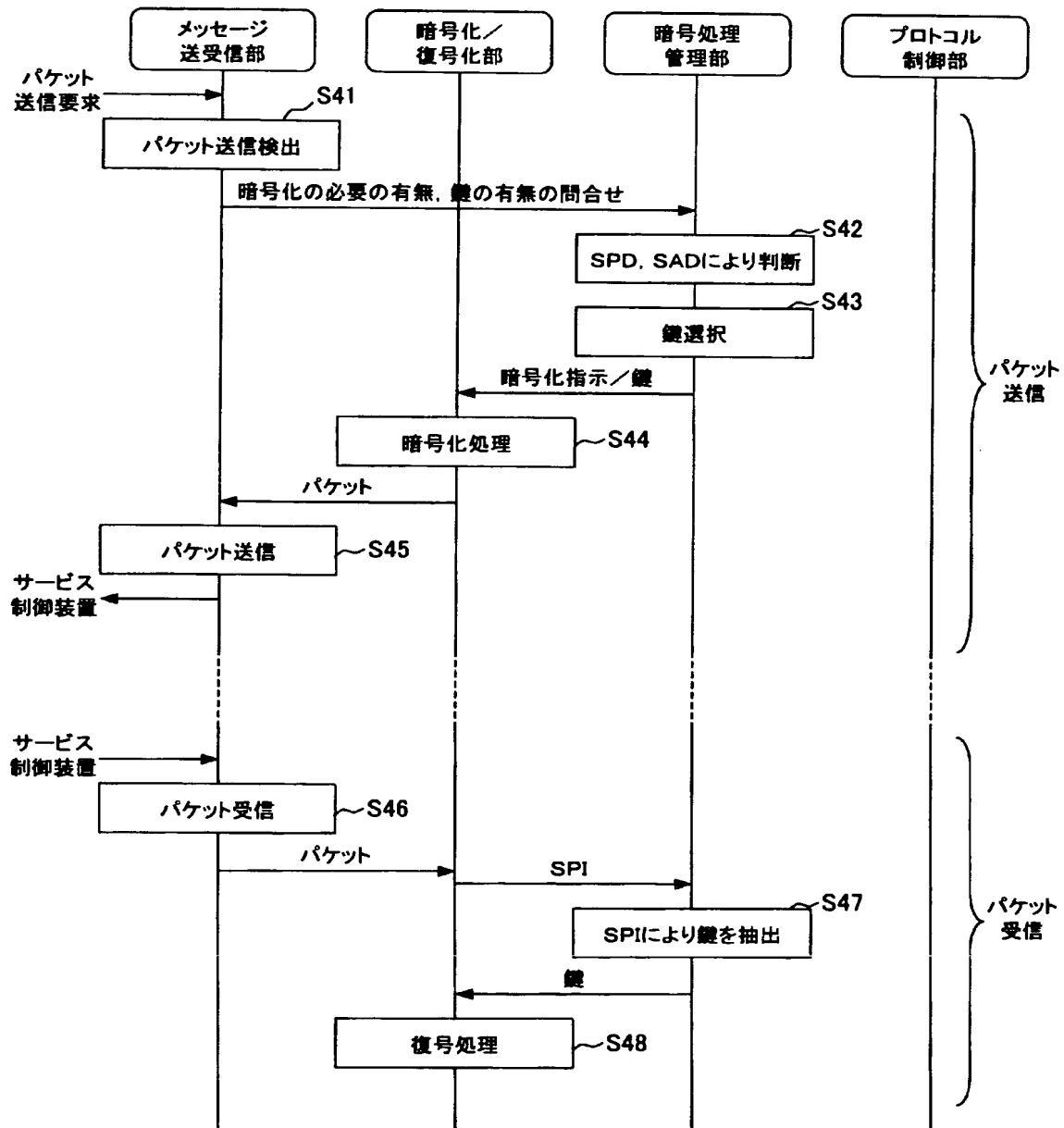
IPヘッダ SA: 鍵交換代理サーバ DA: サービス制御装置	IPヘッダ SA: 通信相手端末 DA: 加入者端末	鍵情報(SA)
---------------------------------------	----------------------------------	---------

## (B) 鍵転送メッセージ

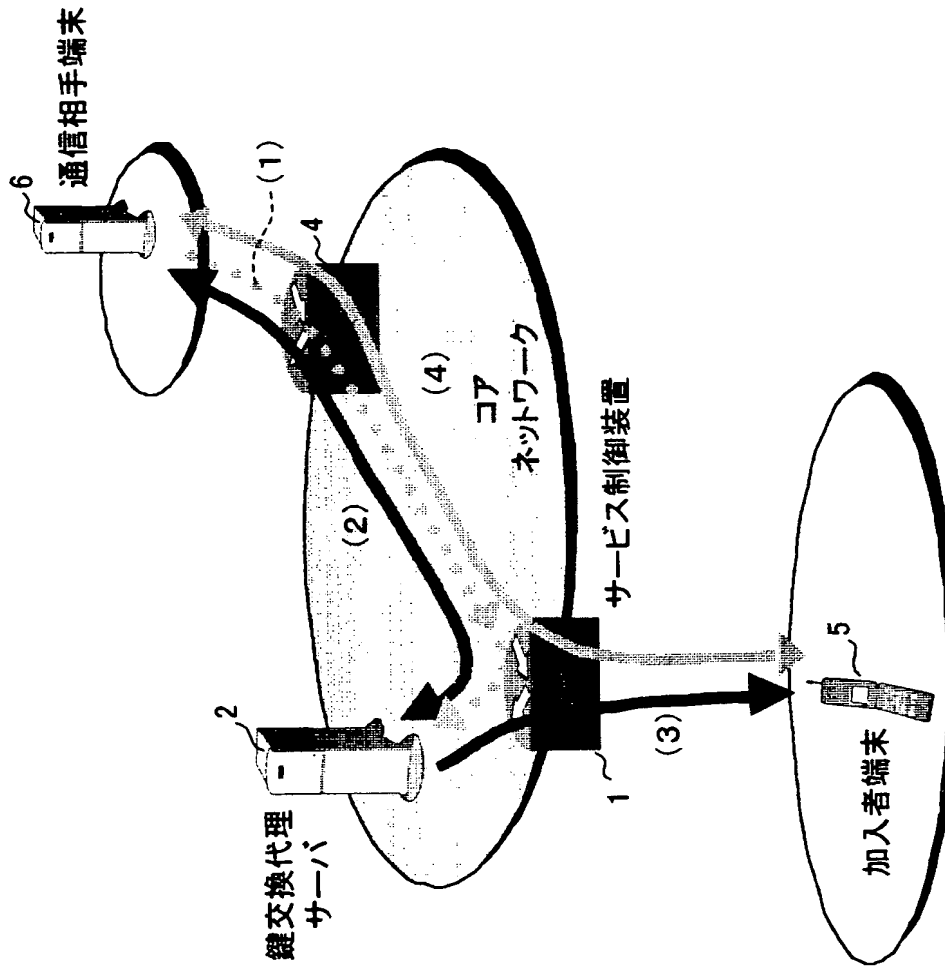
(サービス制御装置→加入者端末)

IPヘッダ SA: サービス制御装置 DA: 加入者端末	IPヘッダ SA: 通信相手端末 DA: 加入者端末	鍵情報(SA)
------------------------------------	----------------------------------	---------

【図 15】

加入者端末の処理シーケンス  
(パケット送受信)

【図 16】



【書類名】 要約書

【要約】

【課題】 鍵交換に伴う処理をネットワーク側の装置に代行させて、端末の負荷を軽減する。

【解決手段】 加入者端末 5 は、通信相手端末 6 との間で行う通信の暗号化に必要な暗号鍵を保持しない場合に、鍵交換代理要求メッセージをサービス制御装置 1 に送信する。サービス制御装置 1 は、認証サーバ 3 から与えられたサービスプロファイルに基づいて、鍵交換代理要求メッセージを鍵交換代理サーバ 2 に転送する。鍵交換代理サーバ 2 は、鍵交換メッセージを通信相手端末 6 との間で送受信して鍵を決定し、決定した鍵を含むメッセージをサービス制御装置 1 に送信する。サービス制御装置 1 は、鍵交換代理サーバ 2 からの鍵を含むメッセージをサービスプロファイルに基づいて加入者端末 5 に転送する。その後、加入者端末 5 と通信相手端末 6 との間で、暗号化通信が行われる。

【選択図】 図 1



特願 2 0 0 2 - 2 8 8 4 7 6

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 5 2 2 3 ]

1. 変更年月日

1 9 9 0 年 8 月 2 4 日

[変更理由]

新規登録

住 所

神奈川県川崎市中原区上小田中 1 0 1 5 番地

氏 名

富士通株式会社

2. 変更年月日

1 9 9 6 年 3 月 2 6 日

[変更理由]

住所変更

住 所

神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号

氏 名

富士通株式会社